LAUREA AMMATTIKORKEAKOULU Uuden edellä

Selvitystyö henkilöstötietoturvallisuudesta koulutuksiajärjestävässä organisaatiossa

Tanni, Markku

2010 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Selvitystyö henkilöstötietoturvallisuudesta koulutuksia järjestävässä organisaatiossa

Markku Tanni
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu 2010

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Tiivistelmä

Tanni Markku

Selvitystyö henkilöstötietoturvallisuudesta koulutuksia järjestävässä organisaatiossa

Vuosi 2010 Sivumäärä 43

Tämän opinnäytetyön tarkoitus oli luoda ensimmäinen teoreettinen pohja erään koulutuksia järjestävän organisaation käyttöön. Toiminnallinen opinnäytetyö oli työelämätarpeeseen perustuva selvitystyö, jossa tietopohja koostettiin kirjallisuuskatsauksen ja asiantuntijahaastattelujen avulla. Toimeksiannon tarjonnut yritys oli aktiivisesti mukana työn ohjaamisessa ja antoi jatkuvasti palautetta sen etenemisestä sekä kohdentamisesta.

Opinnäytetyössä ei haluttu rajoittaa lopputuotteen, henkilöstötietoturvallisuuden tarkistuslistan käytettävyyttä sitomalla se johonkin tiettyyn suomalaisen tai kansainvälisen koulutusjärjestelmän tai –sektorin osaan. Kohdeorganisaation toimintaympäristöä tarkkailemalla oli huomattavissa, että koulutus on palvelutuote joka muodostuu lähtökohtaisesti julkisesta tiedosta. Tämä muodostaa haasteita sekä henkilöstön toimintaan liittyvän tietoturvallisuuden suunnittelulle kuin toteutuksellekin.

Ihanteellisessa tilanteessa koulutuksen järjestäjä voi esittää kaiken toimintaansa liittyvän tiedon julkisena. Tällöin organisaation kilpailukyky ei perustu suoranaisesti jonkin tiedon suojaamiseen vaan tiedon, taidon ja asenteen muodostamaan kokonaisuuteen, joka määrittelee kyseistä koulutuksen järjestäjää.

Henkilöstön toiminta voi vaarantaa koulutuksen järjestäjän tietoturvallisuuden. Kohdeorganisaatiossa käytössä olevat sähköiset oppimisympäristöt sekä toimitilojen puolijulkinen luonne asettavat sille omalaatuisia haasteita. Lisäksi lainsäädäntö asettaa tiettyjä koulutuksen järjestäjän toimintaan liittyviä tietoturvallisuuden raameja, kuten esimerkiksi henkilötietojen käsittelyyn liittyvät kysymykset.

Henkilöstötietoturvallisuuden tarkistuslista löytyy opinnäytetyön liitteistä. Sitä voidaan hyödyntää myös muissa koulutuksia järjestävissä organisaatioissa paikallisin mukautuksin varustettuna. Opinnäytetyön varsinaisen selvitystyön ohessa vakiintui tarkastelun käyttöön termi ”henkilöstötietoturvallisuus”.

Asiasanat: Henkilöstötietoturvallisuus, koulutus

Laurea University of Applied Sciences

Laurea Leppävaara
Security Management Programme

Abstract

Tanni Markku

Study of information security concerning personnel in an organisation providing training services

Year 2010 Pages 43

This thesis is a study intended to help an organisation providing educational services to improve its level of information security. Specifically, the focus of observation was on information security concerning activities of the organisation's personnel. The study was conducted by utilising a literary review and interviews in order to attain information and a factual basis for the checklist of information security concerning personnel.

Educational and/or instructional services are a significant part of societies today. Efficient management of information security relies on identification, assessment and evaluation of information assets. Simultaneously training and educational institutions are often supported on both governmental and regional levels. This implies pressure on publishing and distributing all the information they possess regardless of whether it would give them competitive advantages.

In an ideal situation, an organisation providing training or educational services as their core business should be able to publish every piece of information about its activities excluding possible business venture that are under development. Also the national legislation on protection of personal information must be implemented.

Using the checklist found in the appendix section of this thesis, an organisation may begin its development of personnel's information security from the start. Also a more advanced level may also have already been achieved, in which case the checklist may provide useful advice on its enhancement.

The checklist and the gathering of theoretical knowledge behind it are meant to be used in organisations providing educational or training services, i.e. training centres, schools, universities as well as private enterprises.

Keywords: Information Security, training/education, personnel

Sisällys

1 Johdanto

Korkeakoulutuksesta halutaan tehdä 2010-luvulla merkittävä vientituote kuten valtioneuvoston periaatepäätös (2010) kertoo. Korkeakoulutuksen lisäksi maassamme annetaan myös paljon muuta yhteiskunnan tukemaa tutkintoon johtavaa ja johtamatonta koulutusta (Rahoitus – tietoa järjestelmästä 2010). Koulutuksen järjestäjien laatuun ja laatujärjestelmiin kiinnitetään sekä viranomaistoimijoiden että koulutussektorien itsensä toimesta huomiota (Ammatillisen koulutuksen laadunhallintasuositus 2008, 6-10; Auditointeja koskevat julkaisut 2010). Tämän lisäksi oppilaitosten turvallisuuskysymykset ovat viime vuosien kouluampumisvälikohtausten johdosta olleet laajasti esillä, joskin asian johdosta tehdyt selvitykset ovat usein keskittyneet voimakkaasti näkökulmasta riippuen joko henkilö- tai työturvallisuuden viitekehyksiin (Oppilaitosten turvallisuus 2010, 14-22).

Tietoturvallisuutta ei usein mielletä oppilaitosturvallisuuteen kuuluvaksi osa-alueeksi (Tietoturva osaksi kouluturvallisuutta 2010). Tämä siitäkin huolimatta, että tietoturvallisuus tunnustetaan keskeiseksi kokonaisturvallisuuden hallinnan osa-alueeksi (esim. Kyrölä 2001, 11, 27-30; Miettinen 2002, 129-130; Puolustusministeriö 2009). Henkilöstöturvallisuus taas mielletään usein omaksi, käsitteellisesti erilliseksi kokonaisturvallisuuden osa-alueekseen (Miettinen 2002, 103) erillään tietoturvallisuudesta. Käsitteiden rajojen hämäryys vaikeuttaa turvallisuuskysymysten hahmottamista ja painoarvojen määrittelyä koulutusalalla.

Koulutuksen järjestäjien välisessä kilpailussa opiskelijoista ja opiskelijamäärän mukaan myönnettävästä yhteiskunnan rahallisesta tuesta merkittäviä tekijöitä ovat niiden palveluksessa toimiva henkilöstö sekä niiden yksilöllinen tapa järjestää koulutusta (Opetushallitus 2008, 13-15, 22). Tämä tapa yhdessä muiden yksilöllisten tekijöiden kanssa muodostavat tietopääomaa, jota koulutuksen järjestäjän kannattaa suojata siinä missä minkä tahansa muunkin tulevaisuuden toimintaedellytyksistä kiinnostuneen organisaation.

Tämä opinnäyte on selvitystyö, jonka tavoitteena on kehittää erään koulutuksia järjestävän organisaation henkilöstötietoturvallisuutta. Selvitystyön tavoitteena syntyi tarkastuslista henkilöstötietoturvallisuuden kehittämistyön tueksi. Lisäksi muodostettiin kuva siitä, mitkä henkilöstötietoturvallisuuden osa-alueet ovat relevantteja kyseisessä koulutuksia järjestävässä organisaatiossa.

2 Työn tarkoitus ja lähtökohta

Tämä opinnäytetyö on erään ydintoimintanaan koulutuksia järjestävän organisaation (tästedes: Organisaatio X) hyväksi laadittu selvitystyö. Tällä työllä organisaatio X halusi selvittää, miten se voisi kehittää henkilöstönsä toimintaan liittyvää tietoturvallisuutta. Asian tiimoilta

käytiin toimeksiantajan edustajien kanssa kartoittava keskustelu, jonka perusteella opinnäytetyön tarkastelu kohdentui. Toiminnallisen opinnäytetyön laatimisen myötä haluttiin luoda kohdeorganisaatiolle ensimmäinen teoreettinen pohja sen henkilöstötietoturvallisuuden hallinnalle. Tarkastelun kohteena on nimenomaisesti tietoturvallisuus organisaatio X:n toimiessa tiedon soveltamisen kontekstina.

Jotta tässä opinnäytetyössä kuvattu selvitystyö ja siihen liittyvä toiminnan kehittämiseen tähtäävä toimeksianto ovat mahdollisia toteuttaa, on kerätylle tiedolle saatava soveltamisen konteksti, jolla kerätyn tiedon relevanssia ja hyödyllisyyttä voidaan arvioida. Toiminnallisen opinnäytetyön tavoitteena on organisaatio X:n henkilöstöön liittyvän tietoturvallisuuden tilan selvittäminen olemassa oleviin teorialähteisiin verrattuna. On huomioitava, että tämän opinnäytetyöraportin tarkoitus ei ole sinänsä kuvata kohdeorganisaation henkilöstötietoturvallisuuden laadullista tai määrällistä tilaa. Sen sijaan tavoitteena on organisaation toiminnan ja toimintaympäristön kannalta relevantin tiedon tunnistaminen ja sen hyödyntäminen. Tavoitteen toteuttamisen kannalta keskeisessä asemassa ovat toimeksiantajan lausunnot sekä ohjaus työn kuluessa.

Jotta organisaatio voi kehittää henkilöstötietoturvallisuuden tasoaan, täytyy aihealueesta kerättyä teoriaa soveltaen verrata organisaation tilaa ja teoriassa kuvattua tavoitetilaa toisiinsa. Välille jäävän eron kurominen umpeen on organisaation vastuulla ja sen harkinnan mukaan toteutettavissa.

Vaikka toiminnallisessa opinnäytetyössä sen paremmin kuin selvitystyössäkään ei käytetä varsinaista tutkimuskysymystä, käytettiin tämän selvityksen laadinnassa apukysymystä: ”Miten organisaatio X voi parantaa henkilöstötietoturvallisuutensa tasoa?” Vastausta lähdettiin etsimään tietopohjaa keräämällä ja asiantuntijaresursseja hyödyntämällä. Työn tuloksena oli henkilöstötietoturvallisuuden tarkistuslista sekä hyödynnettävissä olevaa tietoa kohdeorganisaation tietoturvallisuusympäristöstä.

2.1 Kansallinen turvallisuusauditointikriteeristö KATAKRI

Kansallinen turvallisuusauditointikriteeristö (tästedes: KATAKRI) ei ole tieteellinen käsite, vaan tiettyä tarkoitusta varten laadittu auditoinneissa käytettävä kriteeristö. Kyseinen kohtuullisen laaja auditointikriteeristö toimi tämän opinnäytetyön runkona sekä käsiteltävien aihealueiden rajaajana. Asiaa käsitellään tarkemmin kappaleessa 3.

KATAKRI on luotu suomalaisten viranomaisten, yksityisen sektorin sekä erilaisten yhteisöjen yhteistyöhankkeena, jonka on tarkoitus muiden turvallisuuden osa-alueiden ohella ottaa huomioon ja täyttää valtionhallinnon asettamat tietoturvallisuusvaatimukset. Kriteeristö on

toimenpide-muotoinen osa 08.05.2008 käynnistettyä Sisäisen turvallisuuden ohjelman toista osaa (STO II). KATAKRI:in perustuvia auditointeja suorittavat nimetyt viranomaiset, joita Suomessa ovat Suojelupoliisi, Puolustusministeriö sekä Viestintävirasto tarkastelun kohteena olevasta organisaatiosta riippuen. Tietoturvallisuuden osalta KATAKRI täyttää kansainvälisen standardijärjestö ISO:n liittyvän ISO 27000-standardiperheen sekä Suomen Valtionhallinnon tietoturvallisuuden ohjausryhmä VAHTI:n tietoturvallisuudesta antamat ohjeistukset (Puolustusministeriö 2009, 1, 57). KATAKRI on opinnäytetyön ymmärtämisen kannalta merkittävä käsite, sillä kriteeristö toimii sekä keskeisenä teoria-aineiston rajaajana että toimeksiannon mukaisena lähtökohtana.

Opinnäytetyöstä rajattiin pois seuraavat KATAKRI:n puitteissa käsitellyt tietoturvallisuuden osa-alueet (2010, 3):

- Hallinnollinen tietoturvallisuus
- Fyysinen turvallisuus osana tietoturvallisuutta
- Tietoliikenneturvallisuus
- Tietojärjestelmäturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus

Rajaus perustui toimeksiantajan tarpeeseen nimenomaisesti tietoturvallisuuden osalta sekä tarveharkintaan siitä, mikä tieto kehittää organisaation toimintaan haluttuun suuntaan. Näin voitiin keskittyä huolellisesti analyysirunkoa – KATAKRI:a - käyttämällä toimeksiantajan kannalta olennaiseen teoriatietoon.

2.2 Mitä henkilöstötietoturvallisuudella tarkoitetaan?

Tässä kappaleessa esitellään henkilöstötietoturvallisuuteen liittyvää aiempaa tutkimusta sekä tietopohjaa, joka muodostaa lähtökohdan opinnäytetyönä suoritettavalle selvitystyölle. Ensimmäiseksi määritellään ne käsitteet, jotka ovat opinnäytetyön ymmärtämisen sekä henkilöstötietoturvallisuuden käsitteen hahmottamisen kannalta keskeisiä. Käsitteiden määritelmät luettuaan lukija voi ymmärtää, mitä termeillä tarkoitetaan ja miten ne ovat opinnäytetyön kannalta relevantteja.

Riski on opinnäytetyön ymmärtämisen kannalta keskeinen termi, sillä opinnäytetyön toiminnallinen osuus on itsessään riskien hallinnassa hyödynnettäväksi tarkoitettu toimenpide. Riskillä tarkoitetaan arkikielessä usein vahingonvaaraa tai vahingonuhkaa, jotka toteutuessaan aiheuttavat yksilölle tai organisaatiolle kielteisiä vaikutuksia. Yleinen riskin määritelmä on

riskin toteutumisen todennäköisyyden ja riskin laajuuden tai vakavuuden summa. (Suominen 1999, 9.) Tietoturvallisuusstandardi CISSP:ssä Krutz ja Vines kuvaavat hyvin samankaltaisen laskentamenettelyn termille *uhka* (2003, 4-5).

Riskienhallinnalla tarkoitetaan niiden toimenpiteiden ja menetelmien kokoelmaa, joilla organisaatiossa riskejä pyritään tunnistamaan, arvioimaan ja hallitsemaan (Mitä riskienhallinta on?, 2010). Suominen muistuttaa riskienhallinnan juurien olevan 1900-luvun alussa Yhdysvalloissa harjoitetusta vahinkoriskien hallinnasta, jolloin toiminnassa korostui nimenomaan vahinkojen todennäköisyyden arviointi sekä hallinta. Nykyään riskienhallinnalla käsitetään yleisesti kaikkiin organisaatiota uhkaaviin riskeihin varautumista. (Suominen 1999, 26-27.) Krutz ja Vines toteavat (2003, 15) riskienhallinnan olevan tietoturvallisuustyön tärkein osa.

Tietoturvallisuustoiminta perustuu riskien arviointiin ja tästä arvioinnista johtuviin johtopäätöksiin, jotka mahdollisesti johtavat erilaisiin riskien hallintaan tähtääviin toimenpiteisiin (Miettinen 1999, 50; myös Heliö 2010). Opinnäytetyössä ei oteta kantaa riskien arviointiin tai –hallintaan liittyviin malleihin, vaan työn lähtökohtana toimii organisaatio X:ssä sellaisenaan vallitseva riskienhallintaympäristö. Opinnäytetyössä käytetään lukijan työn helpottamiseksi termejä riski ja riskienhallinta. Kumpaakin käsitettä käytetään lähtökohtaisesti yritysten ja muiden organisaatioiden, ei yksilöiden näkökulmasta. Asiayhteydestä riippuen riskienhallinnalla voidaan tarkoittaa joko riskien tunnistamista, arviointia tai varsinaisia, näiden vaiheiden jälkeen tapahtuvia toimenpiteitä joilla riski yritetään poistaa, minimoida tai optimoida.

Miettinen (1999, 295) toteaa *tiedon* koostuvan käyttäjälle muodostuvista merkityksistä, joiden rakennusaineen on erin talletus- ja esitysmuodoissa oleva data. ASIS (2007, 7) määrittelee tietoturvallisuuden viitekehyksessä tiedon sellaiseksi aineettomaksi omaisuudeksi, jolla on arvoa omistajalleen. Omaisuusnäkökulmaa kannattavat myös Kyrölä (2001, 71-73) sekä Heliö (2010), jotka pitävät organisaation toiminnan kannalta keskeisten tietojen tunnistamista ja arvottamista keskeisenä tapana aloittaa tietoturvallisuustyö. Synott ja Gruber (1981) käyttävät tiedosta kirjoittaessaan yksinkertaisesti ilmaisua resurssi.

Suojattavalla tiedolla tarkoitetaan sellaista tietoa, johon organisaatio kohdistaa suojaustoimenpiteitä. Tällainen tieto on organisaatiolle arvokasta – sen päätyminen vääriin käsiin voi joko aiheuttaa kilpailuedun menetyksen, maineriskin, suoria taloudellisia vahinkoja tai useita näistä. Keskeistä on, että tietoturvallisuustyö keskittyy nimenomaisesti suojattavaan tietoon. Muuhun tietoon kohdistuvat suojaustoimenpiteet eivät useinkaan ole taloudellisesti järkevää toimintaa. (Heliö 2010 ; Krutz & Vines 2003, 5-7 ; Kyrölä 2001, 24.)

Tietoturvallisuudella tarkoitetaan valtionhallinnon tietoturvallisuussanastossa niiden järjestelyiden kokoelmaa, joilla pyritään varmistamaan suojattavan tiedon *luottamuksellisuus, eheys*

ja käytettävyys (Valtionvarainministeriö 2008b ; Miettinen 1999, 23-24). Laajalti hyväksytyn CISSP (Certified Information System Security Professional)-standardin sisältämän määrittelyn mukaisesti luottamuksellisuudella pyritään varmistamaan se, että suojatun tiedon muodostama sisältö ei päädy kuin sellaisille tahoille, joille sitä ei ole tarkoitettu. Tässä yhteydessä tarkoitetaan sekä tiedon tahatonta että tahatonta paljastumista. Eheydellä tarkoitetaan pelkistetysti sitä, että tiedon sisältöä ei päästä muuttamaan muuta kuin sellaisten tahojen toimesta, joilla on tähän oikeus. Käytettävyydellä taas pyritään varmistamaan, että valtuutetut tahot pääsevät tiedon sisältöihin käsiksi juuri silloin, kun tarve on. (Krutz & Vines 2003, 3.)

Tämän niin sanotun *tietoturvallisuuden kolmiomallin* (engl. *CIA-triad*) mielekkyydestä ja käyttökelpoisuudesta on 2000-luvulla käyty keskustelua jonka tuloksena jotkin tutkijat olisivat siirtymässä useampia tietoturvallisuuden ulottuvuuksia käsittäviin hahmottamismalleihin (esim. Miettinen 1999, 23; Parker 2002). Tästä huolimatta kolmiomallin vakiintuneisuuden vuoksi tässä opinnäytetyössä tietoturvallisuudella tarkoitetaan niiden menetelmien sekä järjestelyiden kokoelmaa, jolla pyritään varmistamaan suojattavan tiedon luottamuksellisuus, eheys sekä käytettävyys. Näihin kolmeen tietoturvallisuustyön tavoitetilaan pyritään erilaisilla menetelmillä, toimilla ja järjestelyillä, joita puolestaan voidaan auditoida erilaisia standardeja tai kriteeristöjä käyttämällä. Riippuen standardin tai kriteeristön tarkastelukohteista, voidaan eri muuttujissa vallitsevia asiantiloja, joiden toivotaan johtavan suojattavan tiedon luottamuksellisuuteen, eheyteen sekä saavutettavuuteen.

Kyrölä huomauttaa (2001,24) että tietoturvallisuustyön tarkoituksenmukaisuuden kannalta myös suojattavan tiedon tunnistaminen on keskeistä (myös: Heliö 2010). Mäkinen (2007, 129-131) käyttää termiä kokonaisturvallisuuden strategia, jossa tietoturvallisuus on yhtenä kokonaisuuden muodostavana klusterina ja jolla on läheinen yhteys turvallisuuskulttuuriin. Tämän näkemyksen etuna voidaan nähdä tietoturvallisuustyön yhteys muihin turvallisuuden hallintaan tähtääviin toimenpiteisiin – tähän pyrkivät myös KATAKRI:n tekijät sekä Kyrölä joka myös yhdistää tietoturvallisuuden osaksi laatujohtamista. (2001, 27-28, 63.)

Valtionvarainministeriön (2008a, 11-12) mukaan *henkilöstöturvallisuudella* tarkoitetaan (organisaation palveluksessa olevista) henkilöistä aiheutuvien riskien hallintaa, erotuksena henkilöstöön kohdistuvien riskien hallinnasta jota vuorostaan tarkoitetaan henkilöturvallisuuden käsitteellä. Valtionhallinnon ohjenuorana toimivassa sanastossaan valtionvarainministeriön (2008b, 33) VAHTI-työryhmä määrittelee henkilöstöturvallisuuden muodostuvan tietoturvallisuuden viitekehyksessä seuraavista osioista:

- Henkilöstön luotettavuus ja soveltuvuus
- Oikeuksien hallinta
- Sijaisjärjestelyt

- Henkilöstön suojaaminen
- Työsuhteen sekä työyhdistelmien järjestelyihin liittyvien turvallisuustekijöiden hoitaminen

Miettinen puolestaan käsittää (1999, 18-19) KATAKRI:ssa esitetyt henkilöstötietoturvallisuuden asiat kuuluviksi termin *henkilöturvallisuus* alle. Tämän hän taas näkee osana käyttämäänsä yrityksen tietoturvallisuuden hahmottamismallia. Miettinen huomauttaa myös, että käsite henkilöturvallisuus on alkujaan peräisin yritysturvallisuuden kokonaishahmottamismalleista (esim. Yritysturvallisuus 2009) kun sillä samanaikaisesti on lukuisia yhtymäkohtia yritysten harjoittamaan tietoturvallisuustoimintaan. Hän erottaa henkilöturvallisuuteen liittyvät ulottuvuuden erillisiksi tietoturvallisuuden osiksi. Mikäli tästä ulottuvuudesta rajataan pois ihmisten (niin organisaatiossa työskentelevien, alihankkijoiden, vieraiden ja muiden sidosryhmien) fyysinen suojaaminen (Miettinen 1999, 161) voidaan hahmottaa KATAKRI:n jaottelun kaltainen henkilöstöön liittyvän tietoturvallisuuden käsite.

Esimerkkeinä henkilötietoturvallisuuteen kuuluvista asioista Miettinen luettelee prosessit joita sovelletaan kun organisaatio rekrytoi uusia ihmisiä, määrittelee uudelleen työntekijöidensä työnkuvia tai päättää työntekijöidensä työsuhteita. Miettinen huomauttaakin henkilöturvallisuustoiminnan tarkoittavan myös henkilöistä johtuvien, tietoon kohdistuvien uhkien torjumista. (Miettinen 1999, 18-19.) Heljaste (2008, 69) toteaakin: *”Ihmiset ovat tosiaan suurin tietoturvauhka”*

Onnistuneen henkilöstötietoturvallisuuden kannalta Miettinen pitää keskeisenä ongelmien ja riskien hallintaa jo ennen niiden ilmaantumista (1999, 161). Samaa ajatusta kannattaa myös Mäkinen (2007, 129.131), joka huomauttaa myös jo realisoituneisiin uhkiin reagoinnin olevan osa tietoturvallisuustyötä. Kyrölä (2001) välttää käyttämästä henkilö- tai henkilöstöturvallisuus-termejä tietoturvallisuuden yhteydessä ja puhuu laajasti tietoriskeistä. Tietoriskeistä kirjoittaessaan Kyrölä viittaa tilanteeseen, jossa liiketoiminnassa tai muussa toiminnassa tarvittava tieto ei ole käytettävissä, se on muuttunutta, vääristynyttä, hävinnyttä tai joutunut vääriin käsiin. Toisin sanoen Kyrölä käsittelee tietoturvallisuutta samoista lähtökohdista kuin CIA-kolmion hyödyntäjät ja lisää mukaan tilanne-aspektin (2001, 25-27). Tässä kategorisoinnissa henkilöstöön liittyvät tietoturvallisuuskysymykset muodostavat yhden osan tiedon olemassaoloon, käsittelyyn ja muihin siihen liittyviin toimiin liittyvistä riskeistä.

Tällaisen käsitteistön käytön heikkoutena voidaan pitää sitä, että lukijalle voi jäädä epäselväksi henkilö- ja henkilöstö(tieto)turvallisuuden eroavaisuudet. Vakiinnuttamalla käsitteistöt saavutettaisiin yhteismitallisuutta standardityössä, mutta silloin vaarana on, että standardeista tulee liian laajoja noudatettavaksi. Tästä käsitteiden yhdenmukaistamiseen liittyvästä ris-

kistä on varoittanut esimerkiksi Laukkala (2010) yritysten kansainvälisen toiminnan riskienhallinnan standardistojen viitekehyksessä.

KATAKRI sisältää osion ”henkilöstöturvallisuus osana tietoturvallisuutta” (Puolustusministeriö 2009, 64-68), joka auditointikysymysten muodossa sisältää seuraavat auditoinneissa tarkasteltavat aihealueet:

- Pääsy- ja käyttöoikeuksien hallinta
- Salassapito- ja vaitiolositoumukset
- Avainhenkilöjärjestelyt
- Organisaation tietoturvaohjeistus, koulutus ja tiedotus
- Tiedon hyväksyttävän käytön säännöt
- Tietoturvaohjeiden noudattaminen ja sen valvonta
- Ulkopuoliset työntekijät sekä vierailijat

Nämä henkilöstötietoturvallisuuden osa-alueet muodostavat teoreettisen tarkastelun viitekehyksen sekä analyysirungon opinnäytetyölle. KATAKRI:n tekijät huomauttavat, että tietoturvallisuuskysymykset menevät usein päällekkäin esimerkiksi fyysisen turvallisuuden tarkastelukohteiden kanssa, eikä tietoturvallisuuskysymyksiä voida tästä johtuen tarkastella täysin erillään kokonaisturvallisuutta arvioidessa. Tämä kuvaa käsitteiden päällekkäisyyttä sekä ongelmallista rajausta varsinkin ajalta ennen KATAKRI:a. (Puolustusministeriö 2009, 57 ; Mustonen 2008, 54.)

Tämän lisäksi voidaan huomata, että henkilöstötietoturvallisuuden käsite on vakiintumaton ja sillä on useita ns. sisarkäsitteitä kuten henkilöstöturvallisuus (British Standards Institution 1995; International Standard Organization 2007). Turha käsitteellisten erojen lietsominen on asioiden hahmottamisen kannalta turhaa, mutta on syytä huomata keskeisimmät erot ja toisaalta ne yhtäläisyydet, joita lähekkäiset termit jakavat.

Käsitteistön yksinkertaistamiseksi tässä opinnäytetyössä käytetään ilmaisua *henkilöstötietoturvallisuus,* jolloin lähtökohtaisesti viitataan KATAKRI:n tarkoittamiin henkilöstöön liittyviin tietoturvallisuuden osa-alueisiin. Näin voidaan välttyä käsitteiden sekoittumiselta toisiinsa ja pystytään erottelemaan toisistaan lukuisat samaa aihepiiriä koskevat käsitteet tietoturvallisuus sekä henkilöstöturvallisuus. Suomen kielitoimisto (2010) ei ole varannut termiä *henkilöstötietoturvallisuus* käytettäväksi minkään tietyn viitekehyksen yhteydessä käytettäväksi.

Kappaleissa 2.2.1 – 2.2.6 kuvataan henkilöstötietoturvallisuuden käsitteen piiriin kuuluvista osa-alueista aiemmin tutkittua tietoa KATAKRI:n muodostaman analyysirungon puitteissa (ks.

luku 3.). Löydetty tieto muodostaa pohjan henkilöstötietoturvallisuuden kehittämiseksi tämän opinnäytetyön kohdeorganisaatiossa.

2.2.1 Pääsy- ja käyttöoikeuksien hallinta

Tietojärjestelmien käyttöoikeuksien hallinnalla pyritään varmistamaan tietojärjestelmien sisältämien tietojen luottamuksellisuus, eheys ja saavutettavuus (Krutz & Vines 2003, 31). KATAKRI:n näkökulmasta (Puolustusministeriö 2009, 64) keskeistä pääsy- ja käyttöoikeuksien hallinnassa on noudattaa yleisesti hyväksi määriteltyjä tiedonhallintatapoja.

Pääsy- ja käyttöoikeuksien hallinta on tässä opinnäytetyössä käsiteltävistä tietoturvallisuuden osa-aluiesta teknisin – hallinnoinnin lisäksi tämän osa-alueen implementointi edellyttää jonkinlaista (tieto)teknistä järjestelmää toimintaympäristökseen. Tämä huomioiden kysymyksessä on kuitenkin KATAKRI:n mukaan nimenomaan henkilöstötietoturvallisuuteen kuuluva asiakokonaisuus, johtuen henkilöstön keskeisestä roolista sen mahdollistajana ja keskeisimpänä riskinä (Kyrölä 2001, 100-101, 182).

KATAKRI edellyttää, että jo lähtötason suosituksia noudattavalla organisaatiolla on olemassa prosessit seuraavien pääsy- ja käyttöoikeuksien hallintaan liittyvien asioiden hoitamiseksi:

- Oikeuden saajan kuuluminen henkilöstöön tai muutoin oikeutettujen joukkoon on varmistettu
- Oikeuksissa tapahtuvien muutosten hallinta on systemaattista ja että muutokset välittyvät tarpeeksi nopeasti esimerkiksi fyysisten ja loogisten järjestelmien välillä.
- Oikeuksien hallinnalla on nimetty vastuuhenkilö sekä ohjeistus, jota prosessiin osallistuvat henkilöt noudattavat
- Käyttö- ja pääsyoikeudet myönnetään työtehtävien muodostamien tarpeiden mukaan.

Perustasolla KATAKRI edellyttää organisaatioilta lähtötason lisäksi seuraavaa:

- Myönnetyt käyttöoikeudet sekä kunkin järjestelmän käyttäjäkanta dokumentoidaan jossakin muodossa
- Järjestelmän käyttäjät ovat listattuina
- Oikeuksia katselmoidaan säännöllisin väliajoin
- Henkilöstöön liittyvien muutosten osalta tieto liikkuu välittömästi tarvittaville tahoille
- Organisaation ulkopuolisen henkilöstön käyttöoikeudet on dokumentoitu erikseen ja dokumenttia pidetään ajan tasalla

(Puolustusministeriö 2009, 64.)

KATAKRI:n listaus pääsy- ja käyttöoikeuksien hallintaan vaikuttavista tekijöistä sisältää sekä hallinnollisia- että loogisia tai teknisiä valvontamekanismeja. Hallinnollisilla valvontamekanismeilla tarkoitetaan järjestelyjä ja menettelyjä tietoon kohdistuvien riskien hallitsemiseksi – tällainen on esimerkiksi linjaus olla antamatta pääsyoikeutta automaattisesti kaikille organisaatiohierarkian mukaan. Loogisilla ja teknisillä valvontamekanismeilla taas tarkoitetaan käytön rajoituksia ja itse tiedon suojaamista esimerkiksi pääsynvalvontaluettelon avulla. (Krutz & Vines 2003, 32.)

Käyttö- ja pääsyoikeuksien hallinnan kannalta olennaista on oikeuksien myöntäminen tarpeen ja työnkuvan, ei organisatorisen aseman mukaan. Riskejä voi muodostua, mikäli organisaatiossa myönnetään tarpeeton määrä oikeuksia automaattisesti esimerkiksi henkilön korkean aseman vuoksi. Pääperiaatteeksi voi omaksua sen, että jokainen organisaation henkilöt eivät tarvitse tietoonsa kaikkea organisaatiossa olevaa tietoa sen paremmin kuin pääsyä kaikkiin tietoihinkaan. (ASIS 2007, 13 ; Kyrölä 2001, 182-183 ; Miettinen 1999, 230-231.)

Miettinen lukee käyttöoikeuksien hallinnan osaksi käyttötoimintojen turvallisuus-nimistä tietoturvallisuuden osa-aluetta. Hän luettelee keskeisiksi käyttöoikeuksien hallinnan perustehtäviksi käyttöoikeuksien luomisen, niihin kohdistuvat muutokset sekä poiston. Käyttöoikeuksien luominen on yrityksen tietojen suojaamisen kannalta kriittisin vaihe – silloin oikeudet saava henkilö pääsee lähtökohtaisesti ensimmäistä kertaa käsiksi organisaation suojattuihin tietoihin. Käyttöoikeuksien luomisessa korostuukin dokumentointi kaikista näkökulmista. On tärkeää, että käyttöoikeuksia myönnetään ainoastaan vakiomuodossa olevan kirjallisen anomuksen perusteella. Muutoin voidaan olla tilanteessa, jossa käyttöoikeuksia myönnetään esimerkiksi puhelinsoittoina tapahtuvien anomisten perusteella. Tällöin tapahtumaketjun selvittäminen jälkeen muuttuu lähes mahdottomaksi kirjallisten todisteiden puuttuessa. (Miettinen 1999, 230-232.)

Miettinen toteaa henkilöstössä tapahtuviin vaihdoksiin, irtisanomisiin ja muihin muutoksiin reagoimisen haasteelliseksi. Organisaation pitäisi pystyä reagoimaan muutostilanteisiin, jotta käyttö- ja pääsyoikeuksia ei jäisi sellaisille henkilöille, joilla ei niitä esimerkiksi irtisanomisesta johtuen enää tulisi olla. Käyttöoikeuksien läpikäymiset, ns. katselmoinnit auttavat ainoastaan, mikäli niitä pystytään järjestämään tarpeeksi usein. Paras vaihtoehto olisi, mikäli automaattisesti työsuhteen tai –tehtävien tilan muuttuessa muutokset pääsy- ja käyttöoikeuksiin tehtäisiin automaattisesti osana prosessia. (Miettinen 1999, 230-232.)

Yhteenvetona voidaan todeta pääsy- ja käyttöoikeuksien hallinnassa olennaisiksi seikoiksi selkeä vastuunjako, prosessimuotoinen ja ohjeistettu oikeuksien hallinta, tarveharkinnan

käyttäminen oikeuksien myöntämisen yhteydessä sekä muutoksiin reagoiminen asianmukaisessa ajassa.

2.2.2 Salassapitosopimukset

Yrityksiä ja muita organisaatioita pyritään Suomessa suojelemaan salassa pidettävän tiedon joutumiselta vääriin käsiin lainsäädännön keinoin. Tällaisesta suojattavasta tiedosta käytetään lainsäädännön puitteissa käsitettä liike-, ammatti- ja yrityssalaisuudet. Työsopimuslain 55/2001 3. luvun 5. §:n mukaan työntekijä on velvoitettu olemaan käyttämättä työnsä kautta saamiaan liike- ja ammattisalaisuuksia omaksi hyödykseen muutoin kun työn suorittamisen kannalta on tarpeen. Lisäksi ns. liike- ja ammattisalaisuuksien ilmaiseminen sivullisille on kiellettyä. Edellä mainitut kiellot koskevat kuitenkin vain ajanjaksoa, jolloin työntekijän työsuhde työantajaansa jatkuu. Mikäli tiedot on hankittu oikeudettomasti, koskee kielto myös työsuhteen jälkeistä aikaa.

Työsopimuslaissa (TSL 55/2001, 3l 5§) viitataan liike- ja ammattisalaisuuksiin sekä niiden salassapitoon. Myös laki sopimattomasta menettelystä elinkeinotoiminnassa (SopMenL 1061/1978) määrittelee neljännessä pykälässään työsuhteen aikana tietoon liikesalaisuuksien hyödyntämisen tai ilmaisun. Käsitteiden liike- ja yrityssalaisuus käyttö niin juridiikassa kuin tietoturvallisuustyössäkin on ongelmallista siksi, että käsitteitä ei ole merkittävällä tarkkuudella määritelty suomalaisessa lainsäädännössä (Skurnik 2004 ; Vapaavuori 2005, 194-195). Asian selkeyttämiseksi on mielekästä puhua suojattavasta tiedosta, jolloin käytetään yleisesti hyväksyttyä ja käytettyä tietoturvallisuuden terminologiaa (Puolustusministeriö 2009, 59; Kyrölä 2001, 80-81; Miettinen 1999, 92).

Työsopimuslaki suojaa organisaatiolle tärkeiden tietojen käyttämistä organisaation etujen vastaisesti ainoastaan työsuhteen vielä jatkuessa. Tämän organisaatioiden toiminnan kannalta vakavan epäkohdan korjaamiseksi laaditaan monissa organisaatioissa salassapito- ja vaitiolosopimuksia. Näissä kirjallisissa sopimuksissa sovitaan (esimerkiksi) työnantajan ja työntekijän välillä siitä, mikä osa jaettavasta tiedosta on salassa pidettävää tietoa, miten tällaista tietoa tulee käsitellä, millä edellytyksillä sitä voidaan hyödyntää ja mihin tarkoitukseen. Lisäksi salassapitosopimuksessa voidaan sopia mahdollisesta vahingonkorvausvelvollisuudesta sekä salassapitoajasta. (Keksintösäätiö 2010.) Solmittava sopimus voi olla voimassa määräajan tai jatkuvasti. Onkin ollut tyypillistä, että lähtökohtaisesti sopimuksella asetetaan yksittäiselle työntekijälle salassapitovelvoite koko loppuelämän ajaksi (Miettinen 2002, 118)

Salassapitosopimusten yleisyyttä on viime aikoina käsitelty julkisuudessa kriittisesti. On esitetty arvioita siitä, että työnantajat pakottaisivat työntekijöitään allekirjoittamaan salassapitosopimuksia jopa sellaisissa työtehtävissä, joissa käsiteltävien tietojen puolesta tämä ei olisi

tarpeellista. (Salassapitosopimukset leviävät yhä useammille aloille 2010.) Yritysten lisäksi myös julkishallinto hyödyntää salassapitosopimusten suomia mahdollisuuksia. Valtionvarainministeriön VAHTI-ohje (2008a, 13) sisällyttää salassapitosopimukset kiinteäksi osaksi julkishallinnon henkilöstöön liittyviä prosesseja.

Kriteeristössä käytetään hieman ristiin käsitteitä salassapitositoumus ja salassapitosopimus. Keskeinen eroavaisuus näiden kahden välillä on se, että salassapitositoumuksen allekirjoittaa vain suojattavaa tietoa vastaanottava osapuoli (Vapaavuori 2005, 161).

Miettinen (2002, 117-118) katsoo salassapitositoumuksiin liittyvät asiat koko yritysturvallisuuden näkökulmasta kuuluvaksi lähtökohtaisesti henkilöturvallisuuden käsitteen alle tietoturvallisuuden asemesta (ks. kappale 2.2.). Hänen mukaansa yrityksen ja yksityisen henkilön välillä solmitut salassapitosopimukset muodostavat sopimustasoisen perustan henkilöturvallisuuden toteuttamiselle sopimustasolla. (Miettinen 2002, 118.)

KATAKRI:n perustason vaatimuksena organisaatioille mainitaan se, että kaikki työntekijät, alihankkijat, ulkopuoliset käyttäjät sekä muut sidosryhmät allekirjoittavat salassapito- tai vaitiolosopimuksen ennen kuin heille annetaan pääsy luottamukselliseen tietoon (Puolustusministeriö 2009, 65). Tästä näkökulmasta tarkasteltuna salassapitosopimuksilla on läheinen suhde käyttäjäoikeuksien hallintaan (ks. edellinen kappale). Käyttöoikeuksien myöntämisprosessi on siis laadittava niin, että myöntäjällä on varmuus salassapitosopimuksen olemassa olemasta ennen oikeuden myöntämistä.

Skurnik suosittelee (2004), että salassapitosopimuksen rikkomisen sanktioksi määriteltäisiin erillinen sopimussakko. Tätä perustellaan sillä, että ainoastaan vahingonkorvauksiin rajoittuvassa sanktiossa vahingon laajuus ja rajallinen arvo on usein mahdotonta näyttää toteen. Sopimusten laatijan eli työnantajan on huolehdittava sopimusta laatiessaan, että sopimustekstiin ei jää tulkinnanvaraa. Epäselvissä tapauksissa salassapitosopimuksissa on kuitenkin työnantajan näkökulmasta myös merkittävä heikko kohta - työnantajalla on näyttövelvollisuus siitä, että työntekijä olisi vuotanut yrityksen suojattavaa tietoa sivullisille. Riippuen tapauksesta, tällaista näyttöä ei välttämättä ole helppoa osoittaa. (Skurnik 2004.)

KATAKRI:n mukaan salassapitosopimuksen perustana ovat yrityksen tiedon suojaamisen tarpeet (Puolustusministeriö 2009, 65). Salassapitosopimuksien olemassa ololla ei ole itseisarvoa vaan niillä pyritään tiedon tarkoituksenmukaiseen suojaamiseen. Liian laveat rajaukset salassapitosopimuksen tekstissä (esim. luokitellaan kaikki yrityksen palveluksessa saatu tieto salassapitositoumuksen piiriin kuuluvaksi) voivat jopa vähentää niiden vaikuttavuutta (Skurnik 2004). Toisaalta esimerkiksi ASIS (2007, 23) kehottaa sopimaan sisällyttämään kaiken liiketoimintaa koskevan tiedonvaihdon salassapitosopimuksen piiriin alusta alkaen, jolloin vältytään

tulkinnanvaroilta. Vapaavuoren mukaan yritysten välillä solmittavat työehtosopimukset (jotka eivät varsinaisesti ole tämän opinnäytetyön aiheena) tulisi muotoilla siten, että ainoastaan ne suojattavaa tietoa vastaanottavan yrityksen työtekijät, jotka tietoa työssään tarvitsevat ovat oikeutettuja saamaan tietoa. Onkin tärkeää, että salassapitosopimuksia keskenään solmivat organisaatiot tuovat nämä asiat riittävän selvästi työntekijöidensä tietoon. (Vapaavuori 2005, 216-218.)

Lukijan on syytä huomioida keskeiset erot suomalaisessa ja yhdysvaltalaisessa liiketoimintafilosofiassa ja –lainsäädännössä arvioidessaan näitä vaihtoehtoja. Tämän opinnäytetyön tarkastelun kohteena ovat lähtökohtaisesti suomalainen toimintaympäristö lainsäädäntöineen.

Yksittäisen sopimuksen kattavuuden lisäksi on muistettava ulottaa sopimukset kaikkiin mahdollisiin toimijoihin, jotka pääsevät suojattavaan tietoon käsiksi. Tämä tulee kysymykseen esimerkiksi liiketoiminnassa, jossa käytetään runsaasti ketjutettua alihankintaa. Salassapitosopimusten on katettava tällaisessa toimintaympäristössä kaikki alihankintaketjun osat organisaatioineen sekä henkilöstöineen. (Puolustusministeriö 2009, 65.)

Voidaan todeta, että salassapitosopimuksen muotoseikkoja, sopimussakon suuruutta määrittelevää eurolukumäärää tai muita nyansseja tärkeämpää on niiden olemassaolo ja kattavuus. Sopimuksen tarkoitus on tehdä allekirjoittaville osapuolille selväksi, mikä tieto on salassa pidettävää sekä mitä tiedon vuotamisesta sivullisille voi seurata. On myös syytä muistuttaa salassapito- ja vaitiolosopimuksien olevan vain juridinen keino jolla pyritään ehkäisemään suojattavien tietojen vuotamista sivullisille – varsinainen toiminnan este sopimus ei ole.

2.2.3 Avainhenkilöjärjestelyt

Erityisesti henkilöstömäärältään pienissä organisaatioissa avainhenkilöriskit ovat usein merkittäviä. Avainhenkilöllä tarkoitetaan henkilöstön jäsentä, jonka tietojen, taitojen ja kokemuksen menettäminen haittaisivat organisaation toimintaa vakavasti. Syy tälle voi esimerkiksi olla se, että kukaan muu organisaatiossa ei yksinkertaisesti kykene hoitamaan avainhenkilön tehtäviä mikäli tämä syystä tai toisesta ei enää olisikaan organisaation käytettävissä. Avainhenkilöys voi muodostua monenlaisista asioista kuten kyseisen henkilön tiedoista, taidoista tai kokemuksesta, esimiestaidoista, kontakteista, omistajuudesta suhteessa organisaatioon ynnä muista yksilöllisistä tekijöistä. Yhteistä näille on se, että organisaation toiminta häiriintyy huomattavasti ilman näitä avainhenkilön henkilökohtaisia ominaisuuksia. (Avainhenkilöt 2009; Avainhenkilöiden työmotivaatio 2009.)

Avainhenkilöt voivat sijaita millä organisatorisella tasolla hyvänsä - ryhmään voivat kuulua niin yrityksen toimitusjohtaja tai keskeistä tietoa tai asiakaskontakteja hallitseva asiantuntija. Tämän lisäksi avainhenkilöitä voi sijaita myös organisaation rajojen ulkopuolilla alihankki-

jan tai yhteyshenkilöiden muodossa, joskaan tämä ei vaikuta merkittävästi avainhenkilön hallussa olevan tiedon suojaamiseen. (Miettinen 1999, 171.)

Merkille pantavaa on se, että esimerkiksi arvostettu PK-RH-foorumi käsittää avainhenkilöjärjestelyt kuuluvaksi henkilö-, ei tietoriskien kategoriaan (Avainhenkilöt 2009). KATAKRI puolestaan lukee avainhenkilöjärjestelyt osaksi henkilöstötietoturvallisuuden kenttää (Puolustúsministeriö 2009, 65).

VAHTI-työryhmä kehottaa organisaatiota luomaan käsityksen organisaatiossa olevista avainhenkilöistä arvioimalla toimenkuvien *kriittisyysasteen*. Tämän jälkeen toimenkuvista löydettyä kriittistä tietoa on levitettävä organisaatioon varahenkilöille siten, että avainhenkilöys lakkaa olemasta. (Valtionvarainministeriö 2004, 43) Tätä lähestymistapaa voidaan kritisoida sillä, että se ei ota huomioon muuttuvia tai dynaamisia, ns. käytännön elämän toimenkuvia. Käytännön keinoiksi avainhenkilöihin liittyvien riskien hallitsemiseksi VAHTI-työryhmä luettelee varahenkilöjärjestelmät, avainhenkilöiden käytettävyyden varmistamisen kaikissa oloissa sekä poikkeustilanteita varten suunnitellun harjoittelun (Valtionvarainministeriö 2007, 57).

Avainhenkilöiden keskuudessa on otettava huomioon riski väärinkäytöksistä. Avainhenkilöllä voi usein olla laajoja tietojärjestelmien käyttöoikeuksia (ks. kappale 2.2.1) organisaatiossa (Miettinen 1999, 171). On myös liike- ja ammattisalaisuuksien näkökulmasta (katso kappale 2.2.2.) tyypillistä, että toiminnalle keskeisen arvokas avainhenkilö siirtyy kilpailevan organisaation palvelukseen tai yksityiseksi yritykseksi (Vapaavuori 2005, 2).

Myös Kyrölä muistuttaa niin avainhenkilöiden kuin muidenkin vastuuasemaltaan keskeisten henkilöiden väärinkäytösten mahdollisuudesta. Vaikka Kyrölän ajatus keskittyykin esimerkiksi hankintapäätöksissä tehtävästä vaikuttamisesta tai organisaatioiden varojen kanavoimiseksi muihin käyttötarkoituksiin kuin mihin ne on tarkoitettu, on vastuuaseman väärinkäytön mahdollisuus syytä ottaa huomioon avainhenkilöjärjestelyjä suunniteltaessa. (Kyrölä 2001, 91.)

Miettinen luettelee avainhenkilöihin liittyvien riskien hallinnan kannalta oleelliseksi sekä avainhenkilöä rekrytoidessa että tämän työsuhteen päättyessä. Rekrytointivaiheessa keskeistä on henkilön soveltuvuuden varmistaminen sekä taustatietojen tarkastaminen. Näiden menetelmien luotettavuus ja tarkoituksenmukaisuus tiedon suojaamisessa riippuu siitä, millaisia järjestelyjä taustojen tarkistamiseksi ja soveltuvuuden arvioimiseksi toteutetaan. (Miettinen 1999, 171-172.)

Valtionhallinnon tietoturvallisuuden arvioinneissa huomautetaan, että avainhenkilöiden työtehtäviin liittyvät ns. ”vaaralliset työyhdistelmät” ovat organisaation tiedossa (Valtionvarainministeriö 2006). Tällä tarkoitetaan tilannetta, jossa esimerkiksi sama organisaatioon kuuluva

henkilö valvoo tietojen käyttöä tietoturvallisuuden näkökulmasta sekä itse käyttää samaisia tietoja toisena työtehtävänään. Tällöin kyseisellä henkilöllä on mahdollisuus esimerkiksi kopioida luvattomasti organisaation suojattuja tietoja itselleen ilman, että kukaan muu tätä havaitsee. (Miettinen 1999, 171.) Kyrölä huomauttaa, että tällainen tilanne voi myös koskea useampaa ihmistä, joiden työtehtävät mahdollistavat vilpillisen tai laittoman toiminnan. Käyttökelpoinen hallintakeino tälle tietoturvallisuusriskille on tällaisten työtehtäväyhdistelmien kartoittaminen ja sitä kautta väärän toiminnan mahdottomaksi tekeminen. (Kyrölä 2001, 85-86.)

Avainhenkilöjärjestelyiden lukeminen osaksi henkilöstötietoturvallisuutta ei ole itsestään selvä valinta. Niiden lukeminen osaksi tietoturvallisuustyötä perustuu siihen, että avainhenkilöillä on hallussa organisaation toiminnan kannalta kriittistä tietoa (Puolustusministeriö 2009, 65). Tästä voidaan johtaa yhtymäkohtia muun muassa salassapitositoumusasioihin (ks. edellinen kappale), sillä kriittisen tiedon vuotamisen riski voi kasvaa, mikäli avainhenkilö on tiedon ainoa omistaja ja/tai hyödyntäjä organisaatiossa. Keskeisenä keinona avainhenkilöihin liittyvien tietoriskien hillinnässä nähdään yleisesti toimivan varahenkilöjärjestelmän aikaansaamista. Lisäksi on huolehdittava avainhenkilöiden ja heidän varahenkilöidensä osaamisesta organisaation kriittisten toimintojen osalta niin normaali- kuin poikkeusolosuhteissa.

KATAKRI ei sisällytä rekrytointitilanteeseen tai irtisanomiseen liittyvää tietoturvallisuustyötä osaksi henkilöstötietoturvallisuuden tarkastelua, vaan käsittelee sitä yleisiä henkilöstöriskejä käsittelevässä osassa. Kysymys lienee lähinnä eroista siinä, hahmotetaanko henkilöturvallisuus myös osaksi tietoturvallisuutta (Puolustusministeriö 2009, 38-43, vrt. Miettinen 1999 171-172). Kysymyksessä on jo aiemmin tunnistettu ongelma käsitteiden määrittelyssä ja niiden tosielämässä esiintyvässä osittaisessa päällekkäisyydessä (ks. kappale 2.2).

2.2.4 Ohjeistus, koulutus, tiedotus

KATARKI:n määrittelemällä perustasolla (IV) organisaation henkilöstötietoturvallisuustoiminnassa esiintyvät seuraavat asiat:

- Turvallisen käytön ohjeistukset salassa pidettävää tietoa sisältävien järjestelmien käyttöön
- Tiedon tietoturvaluokittelua, tiedon käsittelyä sekä tallennusta koskeva ohjeistus on laadittu ja otettu käyttöön
- Henkilötietojen käsittelystä ja näihin liittyvästä vastuusta on annettu ohjeistus ja annettu asiaan liittyvä perehdytys

- Henkilöstö on ohjeistettu sekä velvoitettu ilmoittamaan havaitsemistaan tietoturvallisuuspoikkeamista ja –uhkista
- Työasemien tietoturva-aukkojen päivittämisestä annetaan varoitus etukäteen ja henkilöstö tietää etukäteen miten toimia päivityksiin liittyen
- Henkilöstölle tiedotetaan ajankohtaisista tietoturvallisuusuhkista, jotka koskevat merkittävästi heidän työskentelyään ja jotka koskevat yrityksen suojattavaa tietoa

(Puolustusministeriö 2009, 66.)

Tietoturvallisuuteen liittyvään ohjeistukseen, koulutukseen ja tiedotukseen löytyy kattavia laatimisohjeita lukuisista eri lähteistä. Haasteena onkin tarkentaa, mitä tietoturvallisuuteen kuuluvia aihealueita näiden tulisi kattaa. Onkin mielenkiintoista, että KATAKRI:n tekijät luokittelevat asian henkilöstötietoturvallisuuteen eivätkä hallinnolliseen tietoturvallisuuteen liittyviksi asioiksi. Aluksi on syytä hahmottaa mitä termeillä ohjeistus, koulutus ja tiedotus tarkoitetaan henkilöstötietoturvallisuuden kontekstissa.

KATAKRI:n mukaan henkilöstölle on annettava riittävä ohjeistus tietoturvallisuuteen liittyvistä asioista (Puolustusministeriö 2009, 66). Perustason vaatimuksista käy ilmi, mitä funktioita ohjeistuksen on koskettava, mutta kriteeristö ei ota kantaa aiheista annetun ohjeistuksen syvällisyyteen tai muotoon.

Tietoturvallisuusohjeistuksesta puhuttaessa on mahdotonta sivuttaa tietoturvallisuuspolitiikkaa, joka KATAKRI:n tarkastelurungossa sijoittuu hallinnollisen- eikä henkilöstötietoturvallisuuden alle (Puolustusministeriö 2009, 58-59). Ohjeistukset ovat jalkautuskeino organisaation tietoturvallisuuspolitiikalle, jossa yrityksen johto määrittelee linjauksensa yrityksen tavasta hoitaa tietoturvallisuuttaan (Krutz & Vines 2003, 11 ; Miettinen 1999, 104-105, 145-147). Miettisen mukaan tietoturvallisuuspolitiikan- ja ohjeiden mukaan sijoittuvat tietoturvallisuusstandardit, jotka kuvaavat toimintamalleja, joilla yritys toteuttaa tietoturvallisuuspolitiikkaa (Miettinen 1999, 104-105).

ASIS käyttää tietoturvallisuuspolitiikan kaltaisesta peruskirjasta englanninkielistä ilmaisua *Information Asset Protection Policy* (suom. Tieto-omaisuuden suojaamispolitiikka), jossa korostuu tiedon omaisuusnäkökulma (ASIS 2007, 8-9). Tässä opinnäytetyössä ei keskitytä tietoturvallisuuspolitiikkoihin tai sellaisten sisältöihin, mutta lukijan on hyvä tiedostaa, että politiikat ovat keskeisenen osa tietoturvallisuuden hallintaa.

Heljasteen (2008, 72) mukaan tietoturvallisuusohjeiston on oltava mahdollisimman lyhyt, käytännöllinen ja mahdollisimman selkeä. Muussa tapauksessa on vaarana, että ne jäävät pölyttymään intranetin syövereihin ilman, että kukaan perehtyy niihin.

Kyrölä suosittelee valmistelemaan tietoturvallisuusasioihin liittyvän ohjeistuksen yhdessä henkilöstön kanssa. Tarkoitus on saada ohjeiden laatimiseen mukaan ne ihmiset, joiden on tarkoitus niitä myös noudattaa. Tietoturva-asiantuntijoiden tai täysin ulkopuolisten henkilöiden käyttäminen tietoturvallisuusohjeiden laatimiseen ilman, että yrityksen henkilöstö on työssä mukana, ei suositella. Kyrölä varoittaa myös riskienhallintaan liittyvien ohjeiden irrallisuudesta ja suosittelee, että ohjeistus koottaisiin käsikirja-tason dokumentiksi. (Kyrölä 2001, 158.)

Turvallisuuskoulutusten järjestämisestä on kirjoitettu ja aihetta on tutkittu runsaasti. Samoin asiaan liittyvän ohjeistuksen antaminen on yritysturvallisuustoiminnan jalkauttamisen kannalta keskeisessä asemassa. (Puhakainen 2009.) Opinnäytetyön toimeksiannon ja KATAKRI:n viitekehyksen kannalta on mielekästä, että tarkastelu rajataan ainoastaan spesifisti tietoturvallisuusasioista annettuun koulutukseen.

Huolimatta siitä onko yritys vahvistanut itselleen kirjallista tietoturvallisuuspolitiikkaa, on ohjeistus keskeisessä osassa kaikkia tiedon suojauskeinoja implementoitaessa. *Tietoturvallisuuskoulutus* on puolestaan työväline, jolla ohjeistus voidaan ja tulisi jalkauttaa yrityksen henkilöstölle (ASIS 2007, 14 ; Miettinen 1999, 158-159 ; Puhakainen 2009.) Kriteeristö ei ota tarkkaa kantaa siihen, mitä tietoturvallisuuteen liittyviä asioita henkilöstölle tulee kouluttaa, vaan mainitsee esimerkkeinä tärkeimmät toimintatilanteet kuten perus- ja etäkäytön, matkatyön ja ylläpidon. (Puolustusministeriö 2009, 58-63, 66.)

CISSP-standardikokeeseen valmistava oppimateriaali käyttää lomittain termejä ”koulutus” ja ”valmennus” puhuessaan tietoturvallisuusohjeiden jalkauttamisesta henkilöstön tietoon. Hyväksi lähtökohdaksi todetaan organisaatiossa käytössä olevien ohjeiden ja vallitsevan toimintaympäristön käyttäminen koulutuksen elävöittäjänä. Itse koulutuksen tarkoituksena on kokonaisturvallisuustietouden paraneminen oikeiden menetelmien ja toimintatapojen oppimisen lisäksi. (Krutz & Vines 2003, 26.)

Puhakaisen näkemyksen mukaan ihmisten motivointi ja rooli turvallisuuden on jäänyt suomalaisessa turvallisuustoimintaympäristössä liian vähälle huomiolle. Tietoturvallisuuden johtamismalleja tutkinut Puhakainen on huomannut organisaatioiden antavan usein liian yleisellä tasolla asioita käsittelevää turvallisuuskoulutusta – tällainen koulutus muodostuu usein turhaksi investoinniksi. (Puhakainen 2009.) ASIS:kin muistuttaa kohderyhmän mukaan tapahtuvan koulutuksen räätälöinnin olevan tärkeää, muuta toisaalta väittää turvatietoisuuskoulutusten (security awareness training) olevan kustannustehokkaimpia tapoja tieto-omaisuuden suojelemiseksi organisaatioissa (ASIS 2007, 14).

Miettinen määrittelee hyvän tietoturvallisuuskoulutuksen laadukkaaksi, jatkuvaksi ja säännölliseksi. Hän mainitsee tietoturvallisuuskoulutuksen perussisällöiksi seuraavat asiat:

- Tietoturvallisuuden merkitys oman organisaation liiketoiminnalle
- Peruskäsitteistö
- Tietoturvallisuuden osa-alueet
- Vastuukysymykset
- Oman toimialan erityispiirteet tietoturvallisuuden näkökulmasta
- Työntekijän lähiympäristön tietoturvallisuus (oma työasema, henkilöstötietoturvallisuus jne)
- Poikkeamien, ongelmien ja väärinkäytösten raportointi organisaatiossa

(Miettinen 1999, 158-159.)

ASIS suosittelee tietoturvallisuuskoulutusten järjestämistä myös lähimpien kumppaniyritysten työntekijöille, jotka usein saavat tietoonsa organisaation suojattavaa tietoa. Myös tilapäinen työvoima, alihankkijat, konsultit ja vastaavat tulisi mahdollisuuksien mukaan kouluttaa. (ASIS 2007, 14.)

Koulutuksien sisältömallit voidaan huomata melko samanlaisiksi lähteestä riippumatta. KATAKRI:n tietoturvallisuusohjeistukseen, -koulutukseen ja tiedotukseen liittyvä tarkastelukysymys tasomäärittelyineen kattaa tieturvallisuuskoulutuksesta annettavat koulutussisällöt henkilöstön kannalta keskeisten tietoriskien osalta hyvin. Yhteistä tietoturvallisuuskoulutusta koskevalle kirjallisuudelle ja ohjeistukselle on, että koulutuksen muotoon kiinnitetään tarkkoja sisältövaatimuksia enemmän huomiota. Koulutusten on oltava organisaation omaan toimintaympäristöön räätälöityjä jotta niiden vaikuttavuus paranee.

KATAKRI:n mukaan henkilöstön tulee annetun koulutuksen seurauksena hallita tietoturvallisuuspoikkeamista tehtävien ilmoitukset. Miettisen mukaan tämä on välttämätöntä, jotta toiminta mahdollisessa poikkeustilanteessa ei olisi hallitsematonta ja sattumanvaraista. Keskeistä tietoturvallisuusongelmiin liittyvässä raportoinnissa on menettelyihin liittyvän ohjeistuksen selkeys. Tärkeintä on saada tieto kulkemaan havaitsijalta tietoturvallisuudesta vastaavalle henkilölle asti. (Miettinen 1999, 152-153.)

KATAKRI:n näkökulmasta tietoturvallisuuteen liittyvä *tiedotus* koskee perustason lähtövaatimusten perusteella merkittävimmistä ajankohtaisista uhkista sekä esimerkiksi tietoturvallisuuteen liittyvistä toimista ja päivityksistä tiedottamista (Puolustusministeriö 2009, 66). Tiedotus tuleekin organisoida toimimaan lähes reaaliaikaisesti. Miettinen huomauttaa (1999, 159), että koottujen koulutustilaisuuksien, joissa ajankohtaisista uhkista voisi tiedottaa katta-

vasti koko organisaation henkilöstöä, voidaan yleensä järjestää vain muutaman vuoden välein, jos niinkään usein. Kyrölä (2001, 215) pitää ohjeistuksista ja poikkeustilanteista ilmoittamista keskeisenä esimiehen tehtävänä. Lisäksi hän toteaa (2001, 203) (tietoturvallisuudestakin) tiedottamisen olevan kiinteä osa yrityksen viestintäpolitiikkaa.

2.2.5 Hyväksyttävän käytön säännöt

KATAKRI käyttää henkilöstötietoturvallisuuden tarkastelukysymyksessään I205.0 käsitettä ”hyväksyttävän käytön säännöt”. Kriteeristössä kuvataan sääntöjä (eng. Acceptable use policy) säännöiksi, joissa määritellään, miten ja mihin tarkoitukseen yrityksen tietojärjestelmiä voidaan käyttää. (Puolustusministeriö 2009, 67.) Esimerkiksi valtionhallinnossa on voimassa henkilöstöä koskeva ohje olla käyttämättä työsähköpostia muuhun kuin työhön liittyvään viestintään (Valtionvarainministeriö 2006, 18). Kyrölä mainitseekin työsähköpostiin liittyvät rajanvedon tyypillisimmiksi hyväksyttävän käytön sääntöjen tarkastelukohteiksi organisaatioissa. (Kyrölä 2001, 187.)

Miettinen (1999, 22) perustelee käyttösääntöjen tarvetta sillä, että suojattavaa tietoa sisältäviä järjestelmiä käytetään ainoastaan siihen tarkoitukseen, joka on organisaatiossa hyväksyttyä. Heljaste toteaa, että internet toimii rikollisten keskeisimpiin kuuluvana toimintakenttänä (2008, 75). Tietoturvallisuuden perusasioitakin arvioitaessa on hyvä huomioida pari henkilöstötietoturvallisuuden kannalta keskeistä lähtökohtaa:

- Tätä dokumenttia kirjoitettaessa yleisetkin internetissä leviävät haittaohjelmat kykenevät imuroimaan tietoa käyttäjän koneilta sekä käyttämään koneen internetyhteyden kaistaa laittomiin tarkoituksiin
- Yrityksen koneelta mahdollisesti ladattu tieto ei välttämättä sisällä välitöntä informatiivista arvoa taholle, joka vastaanottaa haittaohjelman keräämää tietoa. Tämä tieto voi olla kuitenkin analysoitavissa ja sillä voi tämän jälkeen olla arvoa esimerkiksi tarjottaessa sitä suojattavan tiedon omistajien kilpailijoille

(Heljaste 2008, 75-80.)

Yllä mainituista syistä on tärkeää, että organisaatio määrittelee hyväksyttävän käytön tietojärjestelmilleen. Hyväksyttävän käytön säännöt voivat olla räätälöityjä tietojärjestelmä- tai kohderyhmäkohtaisiksi (Malli internetin hyväksyttävän käyttämisen säännöistä kouluille 2002 ; Miettinen 1999, 204-207).

Kyrölä viittaa hyväksyttävän käytön sääntöjen puuttumiseen sillä, että moni suojattavaan tietoon kohdistuva riski toteutuu johtuen organisaatioiden työntekijöiden tietämättömyydestä yhdistettynä huolimattomuuteen ja välinpitämättömyyteen. Esimerkkinä tällaisesta tyypilli-

sestä riskistä Kyrölä mainitsee julkiselle parkkialueelle pysäköidyn auton takapenkille jätetyn kannettavan tietokoneen, jonka tietoja ei ole suojattu. Kysymyksessä voi olla tilanne siitä, että organisaatio ei ole määritellyt, että työntekijät eivät saa viedä työkäytössä olevia kannettavia tietokoneitaan kotiinsa tai säilyttää niitä näkyvällä paikalla (esim. auton takapenkki). Toisaalta työntekijä voi olla tietoinen annetusta säännöstä, mutta ei halua/välitä noudattaa niitä. (Kyrölä 2001, 98-99.)

Tietoturvallisuutta kuvaava kirjallisuus ei sisällön osalta juurikaan erottele hyväksyttävän käytön sääntöjä muista tietoturvallisuusohjeista, joita käsitellään edellisessä kappaleessa. Monessa tapauksessa kirjoittajat käsittelevät ainoastaan tietoturvallisuusohjeistusta osana tietoturvallisuuden hallintaa (ks. kappale 2.2.4.) , eivätkä ota erikseen kantaa hyväksyttävän käytön sääntöihin.

2.2.6 Tietoturvaohjeiden noudattaminen ja tietoturvarikkomukset

KATAKRI:ssa käsitellään tietoturvallisuusohjeiden noudattamisen valvominen näiden laatimisesta ja henkilöstön tietoon saattamisesta (ks. kappale 2.2.4.). KATAKRI:n käyttämät lähteet ovat näissä kahdessa kohdassa jotakuinkin identtiset. Perustason vaatimuksissa tarkastelun kohteena olevan organisaation tietoturvarikkomuksen käsittely sekä seuraukset on määritelty ja ne koskevat samanlaisina koko henkilöstöä. (Puolustusministeriö 2009, 67.)

Häiriötön tila, jossa kaikki organisaation toiminta jatkuu päivästä toiseen ilman tietoturvallisuuteen liittyvien uhkien realisoitumista, ei käytännössä jatku koskaan loputtomiin. Tästä syystä yrityksen on laadittava ja perehdytettävä henkilöstölle menettelyt tilanteessa, jossa joku henkilöstöön kuuluva rikkoo tahallisesti tai tahattomasti tietoturvallisuuteen liittyvää ohjeistusta. Menettelyjen laatiminen ja kuvaaminen tärkeää, jotta väärinkäytöksistä seuraavat toimet ovat aiheutuneen vahingon määrään suhteutettuja sekä oikein ajoitettua. (Miettinen 1999, 153.) Tietoturvarikkomuksiin liittyvät menettelyt ja seuraukset on syytä sisällyttää kiinteäksi osaksi organisaatiossa järjestettävää yleistä tietoturvakoulutusta (ks. kappale 2.2.4).

Tässä opinnäytetyössä ei oteta kantaa siihen, mitä minkin vakavuusasteen tietoturvarikkomuksissa tai väärinkäytöstilanteessa pitäisi seurata. Tähän ei yleisesti oteta kantaa myöskään alan kirjallisuudessa, sillä kategorisia ratkaisumalleja jotka koskisivat kaikkia aloja ja tilanteita yhteismitallisesti on vaikea antaa.

Miettisen käsittelyprosessinmallin (1999, 154) mukaan organisaation tulisi puuttua suojattavaan tietoonsa liittyviin väärinkäytöksiin seuraavasti:

- Väärinkäytöksen havaitseminen, jota varten tarvitaan valvontamekanismeja

- Vahinkojen rajoittaminen
- Tapahtuman tutkinta, jolla selvitetään siihen johtaneet syyt ja sen muut vaikuttavat tekijät
- Vahinkojen korjaaminen vastaavien tapahtumien ja vahinkojen estämiseksi tulevaisuudessa

Amerikkalainen ASIS, jonka näkökulma eroaa systemaattisuudessaan suomalaisista väärinkäytöstilanteista, ottaa kantaa lähinnä väärinkäytöksiin jotka ovat johtaneet tahallisiin tai tahattomiin tietovuotoihin. Näistä vuodoista järjestö olettaa pääsääntöisesti seuraavaan kilpailuedun menetystä ja mitattavia vahinkoja, jolloin yrityksen omaehtoinen tutkinta on avainasemassa vahinkovastuun määrittämiseksi ja vastaavien tilanteiden estämiseksi jatkossa. ASIS kehottaa koordinoimaan tapahtumaan liittyvän tutkinnan yhdessä organisaation lakiasiainosaston kanssa. Järjestö kehottaa pitämään väärinkäytösten ja tietovuotojen varalta hyvät suhteet julkiseen valtaan, yksityisiin palveluihin ja tietolähteisiin. (ASIS 2007, 15-16.)

ASIS kehottaa tutkimuksen lisäksi arvioimaan mahdollisimman tarkasti, minkä suuruinen aineellinen vahinko tietoturvarikkomuksesta on seurannut. Tämä auttaa myös vahinkovastuun ja rahallisten seuraamusten määrittelyssä. (ASIS 2007, 15.)

2.2.7 Ulkopuoliset työntekijät sekä vierailijat

Kangas (2009) mainitsee valvomattoman pääsyn yrityksen tiloihin yhtensä tavallisimmista suojattavaan tietoihin liittyvistä riskeistä (myös: Kyrölä 2001, 122-123). Myös ASIS toteaa niin organisaatioiden omissa, kuin myös ns. off-site-tiloissa (kuten messut, näyttelyt, kokoukset muissa kuin omissa toimitiloissa) järjestettävien tapaamisten olleen historiallisesti tyypillisiä luvattomaan tiedonkeräämiseen ja suoranaiseen teollisuusvakoiluun käytettäviä tilaisuuksia (ASIS 1007, 25-26).

KATAKRI:n perustason vaatimuksiin kuuluu, että organisaatiolla on olemassa keinot ja menetelmät yrityksen toimitiloissa liikkuvien ulkopuolisten yritysten työntekijöiden ja vierailijoiden tunnistamiseksi. Menettelyjen tulee olla organisaation henkilöstön tiedossa ja ne sisältävät seuraavat asiat:

- Yrityksen vierailla ei ole mahdollisuutta jäädä isäntäorganisaation ei-julkisiin tiloihin valvomatta
- Organisaatiossa, jonka työntekijät eivät voi suuresta lukumäärästään johtuen tuntea toisiaan tai toistensa työsuhteiden voimassaoloa, ollaan velvollisia käyttämään kuvallisia henkilötunnisteita.

- Henkilöstö osaa reagoida oikein toimitiloissa liikkuvaan vieraaseen henkilöön, jolla ei ole mainittua tunnistetta.

(Puolustusministeriö 2009, 68.)

Mustosen mukaan (2008, 54-56) vierailijoihin liittyvä ohjeistus on osa hallinnollista tietoturvallisuutta, joka on yhdistelmä toimitilaturvallisuutta ja henkilöstön liittyvää tietoturvallisuutta. Jälleen kerran rajat tietoturvallisuuden ja henkilöihin/henkilöstöön liittyvän turvallisuuden välillä ovat epäselviä.

Vapaavuori mainitsee ns. vierailijan salassapitosopimuksen olevan kelvollinen tapa liikesalaisuuksiin liittyvän vähittäissuojan tarjoamiksi isäntäorganisaatioille. Tällainen sopimus voidaan solmia jo silloin, kun vierailijat saattavat jopa lyhyen neuvottelun, esittelyn tai palaverin aikana saada haltuunsa luottamuksellista, suojattua tietoa. (Vapaavuori 2005, 286-287.)

2.3 Henkilöstötietoturvallisuus koulutuksen järjestäjän näkökulmasta

Aikaisempaa tutkimusta koulutusta järjestävien organisaatioiden tarpeisiin on tehty hyvin vähän, jos ollenkaan. Tämä on ymmärrettävää, sillä tietoturvallisuuden kaltaiset laajat tarkastelun kohteet ovat harvoin tutkimuksellisin keinoin helposti kohdennettavissa vain yhteen tai muutamaan soveltamisen kontekstiin. Vaikka useat koulutuksen järjestäjät eittämättä ovatkin valmistelleen tietoturvallisuuteen liittyviä toimintaohjeita, menettelyjä ja prosesseja omaan toimintaansa, ei näitä ole jalostettu laajassa mitassa koko koulutuskentän hyödynnettäviksi malleiksi.

Seuraavassa kuvataan käsitteet, joiden avulla lukija voi hahmottaa millaisessa kontekstissa opinnäytetyön toimeksi antanut organisaatio toimii.

Koulutus

Tilastokeskus (2010b) jakaa suomalaisen koulutuksen seuraaviin koulutussektoreihin:

- Peruskoulukoulutus
- Lukiokoulutus
- Ammatillinen koulutus
- Ammattikorkeakoulukoulutus
- Yliopistokoulutus

Suomessa valtio osallistuu koulutuksen järjestämisestä aiheutuvien kulujen kattamiseen valtionosuusjärjestelmän avulla (Opetushallitus 2010). Valtionosuudet koostuvat käyttökustannusten sekä perustamiskulujen kattamiseen tarkoitetusta avustuksesta ja niistä säädetään yksityiskohtaisesti laissa opetus- ja kulttuuritoimen rahoittamisesta (1705/2009). Tämän lisäksi myös yksityiset tahot voivat halutessaan järjestää koulutusta lähes mihin tarkoitukseen tahansa ilman valtion tarjoamaa rahallista tukea.

Oppilaitos & koulutuksen järjestäjä

Tilastokeskuksen (2010c) mukaan *oppilaitos* on taho, joka pitää yllä oppilaitokseksi kutsuttua hallinnollista yksikköä. Tilastointitarkoituksissa oppilaitokset luetaan *koulutuksen järjestäjiksi*, joilla tilastokeskus tarkoittaa myös sellaisia koulutuksen järjestäjiä jotka eivät täytä oppilaitoksen kriteerejä (Tilastokeskus 2010a). Tällaisia kriteerejä ovat esimerkiksi työnantajarooli, rehtorin tai muun vastaavan johtajan vakanssin olemassa olo sekä julkisen viranomaisen myöntämä rahoitus (Tilastokeskus 2010c). Käsitteistön yksinkertaistamiseksi ja opinnäytetyön käytettävyyden lisäämiseksi tästedes soveltamisen kontekstia käsiteltäessä käytetään ainoastaan termiä ”koulutuksen järjestäjä”. Organisaatio X, joka toimii opinnäytetyön teorian soveltamisen kontekstina, on Tilastokeskuksen tarkoittama koulutuksen järjestäjä. Opinnäytetyö keskittyy ainoastaan koulutusta ydintoimintanaan järjestävään organisaatioon, ei esimerkiksi jollain muulla toimialalla toimivaa organisaatiota joka haluaa järjestää henkilöstölleen jonkinlaista koulutusta.

Tässä opinnäytetyössä keskitytään tarkastelemaan henkilöstöön liittyvää tietoturvallisuutta erään koulutuksen järjestäjän näkökulmasta, sillä se ei sido tarkastelua koulujärjestelmän eri tasoihin. Näin opinnäytetyössä käsiteltävä teoriatieto on hieman yksinkertaisemmin sovellettavissa mihin tahansa koulutusjärjestelmän sektoriin paikallisin mukautuksin.

2.4 Organisaatio X tietoturvallisuusympäristönä

Seuraavassa kuvataan ympäristö ja olosuhteet, joissa organisaatio X hallitsee tietoturvallisuuttaan. Tiedot perustuvat opinnäytetyön tekijän perehtymiseen kohdeorganisaation toimintaympäristöön sekä organisaation tietoturvallisuudesta vastaavien henkilöiden kanssa käytyihin palaverikeskusteluihin (Organisaatio X 2010). Kokonaisvastuu organisaatio X:n tietoturvallisuudesta kuuluu johtaja A:lle. Tietoturvallisuuteen liittyviä käytännön toimia suunnittelee ja toteuttaa päällikkö B, joka toimii organisaation laatupäällikkönä.

Organisaatio X:n johto kokee, että modernissa palveluyhteiskunnassa tieto voi muodostaa koulutuksen järjestäjälle kilpailuetua lähinnä erilaisten liiketoimintaan tai prosesseihin liittyvien oivallusten muodossa. Varsinkin sellaiset koulutuksen järjestäjät, jotka saavat valtiollista

tai alueellista tukea toimintaansa, ovat sosiaalisessa ja yhteiskunnallisessa vastuussa ympäristölleen. Tämän vuoksi yhteiskuntaa yleisellä tasolla hyödyttävän tiedon panttaaminen kilpailuedun saavuttamiseksi on ongelmallista. Tiedon panttaamista korostava toimintakulttuuri voi organisaatio X:n johtajan mukaan kääntyä jopa organisaatiota vastaan. Varsinaisen kilpailuedun koulutuksia järjestävälle organisaatiolle tarjoaa kompetenssi, joka muodostuu tiedosta, taidosta ja asenteista. Osana tätä kokonaisuutta, tietoa pitää määrätyiltä osin suojata. Useimmilla koulutuksen järjestäjillä on hallussaan lainsäädännön perusteella suojattavaa tietoa, kuten henkilörekistereitä. (Johtaja A, 2010.) Myös organisaatio X:n laatupäällikkö B korostaa koulutuksen järjestäjän kannalta tietoturvallisuutta säätelevän lainsäädännön vaatimusten täyttämistä (Päällikkö B, 2010).

Organisaatio X:n johtoon kuuluva johtaja A kuvaa, että koulutusta ydintoimintanaan järjestävälle organisaatiolle tiedon merkitys riippuu koulutettavasta asiasta tai asioista. On eroteltava toisistaan tiedot, joita organisaatio koulutuksen keinoin opiskelijoilleen siirtää ja tiedot, jotka kuvaavat esimerkiksi organisaation tapaa tehdä asioita, sen mahdollisia liiketoimintasuunnitelmia ja niin edelleen. Mikäli opetettava asiakokonaisuus perustuu yksinomaan tietojen siirtämiseen opiskelijoille, ei kyseistä tietoa kannata suojata tietoturvallisuuden keinoin – sen tarkoitus on siirtyä pois organisaatiosta jolloin se ei myöskään itsessään voi muodostaa erityistä liikesalaisuutta tai kilpailuetua organisaatiolle. Johtaja A näkee tietoturvallisuuden muutenkin entistä ongelmallisemmaksi asiaksi palveluyhteiskunnassa, jossa suuri osa elinkeinotoiminnasta perustuu aineettomien palveluiden – kuten koulutuksen - myyntiin. Hänen mukaansa koulutuksen järjestäjän suojattava tieto on pääasiassa tulevaisuuden toimintasuunnitelmia, kuten esimerkiksi liiketoimintastrategioita tai vielä toteutumattomia palvelukonsepteja. Tavoittelemisen arvoinen tila koulutuksen järjestäjälle on se, kun kaikista sen työkseen käyttämistä menetelmistä, prosesseista sekä oppimateriaalista voidaan kertoa kaikki yksityiskohtia myöten julkisena tietona. Toisaalta tiedon arvoa määrittää myös se, onko organisaatio X:n koulutuksina lisäarvoa ostava taho yksityinen henkilö vai esimerkiksi yritysasiakas, joka kouluttaa henkilöstöään. (Johtaja A, 2010.)

Henkilöstöön liittyvän tietoturvallisuuden kannalta organisaatio X:n laatupäällikkö B näkee tietoturvallisuuden teknisen toteutuksen kannalta haasteelliseksi sähköiset oppimisympäristöt. Näiden järjestelmien osalta on huolehdittava esimerkiksi niin asiakkaiden kuin omankin henkilökunnan käyttöoikeuksien ajantasaisuudesta. Monelta osin organisaatio X:n opettama tieto, eli sen asiakkailleen tarjoamat oppimiskokonaisuudet koostuvat geneerisestä tiedosta, joka ei itsessään muodosta huomattavaa kilpailuetua antajalleen. Kuitenkin on tavaiteltavaa myös organisaation maineen kannalta, että esimerkiksi oppimateriaalit pysyvät organisaation sisällä ja ainoastaan niitä tarvitsevien henkilöiden ulottuvissa. (Johtaja A & Päällikkö B 2010.) Esimerkiksi joidenkin oppimateriaalien sisältämien tietojen joutuminen vääriin käsiin voisi aiheuttaa kielteistä julkisuutta organisaatiolle (Päällikkö B, 2010).

3 Selvitystyön toteutus

Tässä luvussa kuvataan opinnäytetyön laatimiseksi käytetyt menetelmät valintaperusteluineen. Ensimmäisenä esitellään Kansallisen turvallisuusauditointikriteeristön rooli analyysin pohjana toimivana runkona. Tämän jälkeen kuvataan menetelmänä käytetty kirjallisuuskatsaus sekä asiantuntijahaastattelut.

3.1 KATAKRI analyysirunkona

Opinnäytetyön toimeksiantajan kanssa käydyissä keskusteluissa ja opinnäytetyön rajausta käsittelevissä palavereissa tuli ilmi, että KATAKRI:n henkilöstöön liittyvä tietoturvallisuus -osion (I200-sarja) tarkastelukohdat (Puolustusministeriö 2009, 57) ovat organisaation henkilöstötietoturvallisuuden hallinnan kannalta keskeisiä aihealueita. Näin opinnäytetyön rajaaminen koskettamaan ainoastaan KATAKRI:ssa mainittuja aihealueita on luonteva ja se rajaa pois huomattavan osan tietoturvallisuuden hallinnassa tarkasteltavia osa-alueita. Tässä opinnäytetyössä ei myöskään käsitellä muita KATAKRIN käsittelemiä turvallisuuden osa-alueita, joita ovat hallinnollinen turvallisuus & turvallisuusjohtaminen, henkilöstöturvallisuus sekä fyysinen turvallisuus.

Koska kysymyksessä on toiminnallinen opinnäytetyö ja työelämän tarpeesta lähtöisin oleva selvitys, ei siihen sovelleta varsinaisia tutkimuksellisia työmenetelmiä (Koski 2007, 82). Selvitystyön pohjaksi on kerätty teoriatietoa erilaisista lähteistä siten, että tieto keskittyy KATAKRI:n määrittelemiin, henkilöstöön liittyviin tietoturvallisuuskysymyksiin. Tietopohjaksi muodostettua tietoa hyödynnettiin asiantuntijahaastatteluissa sekä palaverityössä oleellisten asioiden tunnistamiseksi ja hyödyntämiseksi henkilöstötietoturvallisuuden tarkistuslistassa.

Tietoturvallisuudesta on laadittu lukuisia standardeja, joita organisaatiot voivat käyttää oman tietoturvallisuutensa tilan arviointiin ja kehittämiseen. Esimerkkejä tällaisista standardeista ovat kansainvälisen standardointijärjestö ISO:n 27000-sarjan tietoturvastandardit. Kansallista näkökulmaa edustavat Valtionhallinnon tietoturvallisuuden ohjausryhmä VAHTI:n julkaisemat tietoturvallisuusohjeet ja –sanastot, joilla pyritään paitsi yhdenmukaistamaan myös saavuttamaan tietty vähimmäistaso julkishallinnon tietoturvallisuusasioissa (Tietoturvallisuus 2010). KATAKRI on laadittu siten, että se täyttää ISO- ja VAHTI-standardien vaatimukset ja suositukset. Näin vältytään lukuisten päällekkäisten standardistojen soveltamiselta, mikä muodostunee KATAKRI:n hyödyntäjille eduksi.

KATAKRI:n auditointimekanismi toimii siten, että kutakin tarkateltavaa aihealuetta varten on olemassa oma auditointikysymyksensä – tämä kysymys määrittelee varsinaisen tarkastelun kohteena kulloinkin olevan asian. Tämän jälkeen on annettu sellaiset lähtötason suositukset, joita jokaisen organisaation tulisi noudattaa. Lähtötason lisäksi KATAKRI:ssa luetellaan perustason vaatimukset (IV), korotetun tason vaatimukset (III) sekä korkean tason vaatimukset (II) jokaiselle auditointikysymykselle. Porrastus johtuu KATAKRI:n alkuperäisestä tarkoituksesta, joka on tarjota korkea turvallisuustaso tarkastelunsa kohteelle kansainvälistä, turvaluokiteltua kaupankäyntiä varten.

Tässä opinnäytetyössä käsitellään lähtökohtaisesti ainoastaan kunkin tarkasteltavan aiheen perustason vaatimuksia, jotka ottavat huomioon lähtötason suositukset jo saavutettuina. Tätä perustellaan kustannusten näkökulmasta. Kaikki turvallisuusjärjestelyt tuottavat kustannuksia, jotka eivät välttämättä esimerkiksi suojattavan tiedon arvoon nähden ole kohtuullisia. Organisaation omassa harkinnassa on, kannattaako sen implementoida vielä perustasoa raskaampia (tieto)turvallisuustoimenpiteitä. Tässä työssä keskeistä on riskien tunnistaminen ja arviointi organisaation toimintaympäristössä ja viitekehyksessä (ks. luku 2)

3.2 Tiedon kerääminen kirjallisuuskatsausta hyödyntäen

Kirjallisuuskatsauksen tehtävä on selvittää ja koota aiemmin suoritetusta tutkimuksesta saavutettu tieto joka koskee käsiteltävää aihealuetta. Näin voidaan hahmottaa käsillä olevan tutkimuksen tarpeellisuutta ja asemaa verrattuna aiempiin tutkimuksiin. Lisäksi kirjallisuuskatsaus toimii tietoaineiston keruumenetelmänä. (Hirsjärvi, Remes & Sajavaara 2004, 111-112) Tämän opinnäytetyön puitteissa suoritetulla kirjallisuuskatsauksella muodostettiin asian käsittelyn kannalta keskeinen tietopohja (ks. kappaleet 2.2.1.-2.2.6)

Kirjallisuuskatsauksen tavoitteena oli kerätä tietoa aiheista, joita KATAKRI mainitsee henkilöstötietoturvallisuuden aihealueeseen. KATAKRI:ssa esiintyvistä tarkastelukohteista kerättiin tietoa jotta saavutettiin syvällisempi ymmärrys tarkastelun alla olevista kohteista. Näin luotiin luotettava pohja henkilöstötietoturvallisuuden mallille, jota hyödynnettiin kohdeorganisaatiossa.

Tietoaineiston koostaminen toteutettiin opinnäytetyön osana ja jolla luotiin pohja kohdeorganisaation henkilöstötietoturvallisuuden kehittämiseksi. Koski (2007, 82) erottelee selvitystyön tutkimuksesta siten, että selvitys ei täytä tiedonhankinnan ja menetelmien osalta samoja tieteellisiä kriteerejä kuin tutkimus. Selvitystöillä on kuitenkin olemassa oma paikkansa organisaatioiden kehittämisessä. Tieteellisen tutkimuksen kriteeristö voi esimerkiksi edellyttää, että teoriapohjaa kerätään ainoastaan tieteellisissä julkaisuissa esiintyneistä artikkeleista. Tällainen menettely ei voi tulla kysymykseen silloin kun organisaatio haluaa ketterästi ja

omia tarkoituksiaan varten kehittää toimintansa tiettyä osa-aluetta - Voihan olla, että asiaa ei ole yksinkertaisesti tutkittu tarpeeksi. Tämän lisäksi kysymykseen tulee selvitys- tai tutkimustyön kustannustehokkuus ja lähteiden karsinnan tarkoituksenmukaisuus.

Kuten todettua, koulutuksen järjestäjille räätälöityä tietoturvallisuusteoriaa on olemassa vähän tai ei ollenkaan yleisesti saatavilla. Teorialähteiksi pyrittiin keräämään mahdollisimman paljon kattavia tietoturvallisuuteen liittyviä teoksia, suosituksia, ohjeita ja standardeja. Kattavuutta toteutetaan lähteiden valinnalla – osa teorialähteistä perustuu puhtaasti tietoturvallisuuden ja sen osa-alueiden hahmottamiseen ja käsittelyyn, kun taas osassa tietoturvallisuutta käsitellään osana laajempia turvallisuuskäsityksiä. Lukijan ei pidä olettaa, että tämä tarkoittaa kahden täysin erillisen turvallisuuskäsityksen hahmottavien lähteiden käyttöä. Tarkoituksena oli luoda katsaus samaan asiaa erilaisilta turvallisuusteoreettisen hierarkian tasoilta.

Teoria-aineiston haalimisen jälkeen kerätystä tiedosta on koottu ensimmäinen versio tarkastuslistasta henkilöstötietoturvallisuuden kehittämiseksi kohdeorganisaatiossa. Tarkastuslistassa esiintyvä henkilöstötietoturvallisuusasioiden hahmottamismalli noudattelee toimeksiantajan tahdosta KATAKRI:n henkilöstötietoturvallisuuden osa-alueista muodostuvaa rakennetta – tällä tavoin on saavutettu säästöjä työhön käytetyissä ajallisissa resursseissa kun hahmottamismallia tai sen rakennetta ei tarvinnut laatia alusta asti.

Ensimmäisen version jälkeen siirryttiin asiantuntijahaastatteluiden ja palaverityön pariin. Näillä pyrittiin varmistamaan, että kohdeorganisaation kannalta keskeiset asiat tulevat huomioiduiksi tarkistuslistan lopullisessa versiossa.

3.3 Asiantuntijahaastattelut

Opinnäytetyön toiminnallisena tuotteena laadittu malli on testattu organisaatiossa haastattelemalla avainhenkilöitä sen arvioimiseksi, onko kerätty tieto tarkoituksenmukaista ja hyödyllistä. Asiantuntijoiden lausuntojen perusteella muodostettiin kuva kyseisestä koulutuksen järjestäjästä tietoturvallisuusympäristönä huomioiden henkilöstöön liittyvä rajaus.

Toimintaympäristön yleisen tietoturvallisuusympäristön määrittelyn lisäksi kohdeorganisaatioiden avainhenkilöitä haastateltiin mukautetun teemahaastattelun periaatetta käyttäen. Hirsjärven ja Hurmeen (2008, 66) tarkoittamien teemahaastattelun teemojen kartoittaminen tapahtui KATAKRI:n tarjoamaa rajausta hyödyntäen (ks. kappale 3.1) Haastattelu on laadullinen tiedonkeruumenetelmä, jonka tarkoitus on koota johonkin ilmiöön liittyvää hiljaista tietoa kirjoitettuun muotoon (Vilkka & Airaksinen 2003, 63). Vertaamalla haastattelun avulla kerättyä tietoa kirjallisuuskatsauksella koottuun tietopohjaan pystyttiin muodostamaan käsitys asioiden relevanssista toisiinsa nähden.

Haastatteluissa haluttiin selvittää mikä on organisaation suhde sen suojattuun tietoon. Selvitettäviin asioihin kuului se, onko organisaatio määritellyt suojattavan tietonsa. Lisäksi haastatteluissa kunkin KATAKRI:n tarjoaman analyysirungon kohtaa käsiteltiin relevanssin näkökulmasta – miten kunkin kohdan kuvaamat aiheet näkyvät kohdeorganisaation päivittäisessä toiminnassa ja miten tärkeiksi avainhenkilöt ne kokevat organisaation tietoturvallisuuden kehittämisen kannalta? Tulokset ohjasivat henkilöstötietoturvallisuuden tarkastuslistan mallin rakentamista siten, että hyödyttömiksi koetut asiat jätettiin pois lopullisesta tarkastuslistasta samalla kun keskeiset asiat suuremmalle. Asiantuntijoiden haastatteluissa käytetty pohja on opinnäytetyön liitteenä 2. Asiantuntijahaastattelut toteutettiin aikavälillä kesä-lokakuu 2010.

Koko opinnäytetyöhön liittyvän toimeksiannon ajan hyödynnettiin haastattelujen lisäksi mahdollisuutta kohdeorganisaatiosta lähtöisin olevaan asiantuntijaresurssiin, jonka tarkoituksena oli ohjata työtä oikeaan suuntaan ja varmistaa se, ettei malli sisällä mitään organisaation tarpeiden kannalta epäolennaista. Menetelmän höytynä on se, että teorian hankinta ja hyödyntäminen kanavoituu toimeksiantajan kannalta tarkoituksenmukaiseen suuntaan. Näin saatiin minimoitua turha työ ja annettiin toimeksiantajalle mahdollisuus ohjata työtä haluamaansa suuntaan.

Johtuen kohdeorganisaation anonymiteetistä opinnäytetyön ohjaajalle on toimitettu lista haastatelluista henkilöistä. Lista sisälsi myös kuvaukset heidän organisatorisesta asemastaan sekä henkilöiden vastuista suhteessa tietoturvallisuuteen.

4 Henkilöstötietoturvallisuus organisaatiossa X

KATAKRI:ssa esitetyt henkilöstötietoturvallisuuden osa-alueet koettiin pääsääntöisesti relevanteiksi organisaation X toimintaympäristössä. Seuraavassa kuvataan jokaisen henkilöstötietoturvallisuuden osa-alueen relevanssi ja painotukset organisaatio X:lle. Viimeiseksi kuvataan muut esille tulleet henkilöstötietoturvallisuuden toteuttamismenetelmät, joita organisaatio X:n asiantuntijat halusivat otettavan huomioon.

Käyttö- ja pääsyoikeuksien hallinnassa keskeistä on sähköisten tietojärjestelmien tunnusten hallinta. ”Haamukäyttäjien” aiheuttamat riskit on tunnistettava ja tietojärjestelmien tunnusten katselmoimista säännöllisin väliajoin tulisi harkita. Tämä työ on kuitenkin työlästä eikä sen vastuuttaminen ole yksinkertaista. Luontevimmaksi käyttäjätunnusten katselmoijaksi nähtiin kyseinen tietojärjestelmän pääkäyttäjä. On huolehdittava, että valvontavastuu ei jää määrittelemättä tai hajaannu liikaa esimerkiksi eri tuotteista (koulutuksista) vastaavien henkilöiden kesken – tämä vaikeuttaa kokonaishahmottamisen mahdollisuuksia. Mahdollisuutena nähtiin teknisten ratkaisujen osalta se, että käyttö- ja pääsyoikeudet ovat voimassa määräajan. Tämä poistaa osan henkilöstön tarpeesta huolehtia tunnuksista tai katselmoida niitä.

Muita käyttö- ja pääsyoikeuksiin liittyviä asioita pidettiin luonnollisena osana prosesseja ilman että ne varsinaisesti vaatisivat hallintaa.

Salassapitosopimukset ovat valmiiksi organisaation X:n käytössä – jokaisen rekrytoitavan työntekijän kanssa solmitaan toistaiseksi voimassa oleva salassapitosopimus, joka koskee kaikkia liike- ja ammattisalaisuuksia. Salassapitosopimusten olemassaoloa pidetään organisaation toiminnan kannalta erittäin relevantteina. Monessa tapauksessa se, että henkilö allekirjoittaa salassapitosopimuksen toimii samanaikaisesti orientaationa organisaation tietoturvallisuuskulttuuriin. Vahingonkorvausvastuu rikkomustilanteissa nähdään ongelmalliseksi sen takia, että monikaan organisaation X:n suojattavaksi luokittelemasta tiedosta ei ole rahallisesti arvotettavissa. Tällaisia ovat esimerkiksi tulevat suunnitelmat toiminnan organisoimisesta sekä asiakkaiden sekä henkilöstön omat henkilötiedot. Salassapitosopimuksen solmimisessa tulisi kuitenkin muistaa, ettei se korvaa tiedon luottamuksellisuudesta muistuttamista arkipäivän tilanteissa. Vahingonkorvausvelvollisuuden toteutumisen kriteerien määrittelyä pidettiin ongelmallisena johtuen suojattavan tiedon luonteesta. Korvausvelvollisuuden sitomista sopimussakkoon ei mainittu tarpeellisena tai organisaatiota palvelevana elementtinä.

Avainhenkilöriskit koetaan organisaatiossa huomattavaksi ja niiden hallinta on keskeisessä osassa suunniteltaessa organisaation toiminnan jatkuvuutta. Organisaatio X kokee välttämättömäksi tilanteen, jossa jonkin henkilöstön jäsenen hallussa on tietoa jota ei ole kenelläkään toisella organisaatiossa. Koulutuksen järjestäjän on tunnistettava avainhenkilöriskinsä ja laadittava varahenkilöjärjestelmä. Riskinä koetaan sekä organisaation henkilöstön jäsenten siirtyminen kilpailijoiden tai muiden alojen työntekijöiden palvelukseen. Tässä tapauksessa osaaminen siirtyisi pois ja tilalle olisi äärimmäisen vaikeaa saada osaavaa työvoimaa. Kysymyksessä ei ole niinkään kilpailuedun menettäminen väliaikaisesti kilpailijoille vaan se, että tilalle palkattavan henkilön perehdyttäminen on työlästä. Vaarallisten työnkuvayhdistelmien aktiivista valvomista ei nähty niin olennaisiksi toiminnan luonteen ja olemassa olevien järjestelmienvuoksi. Organisaation jatkon kannalta pidettiin kuitenkin tärkeänä, että mahdollisesti vaarallisten työnkuvien varalta ollaan tarkkoina varsinkin prosesseja muutettaessa ja organisaatiota kehitettäessä. Tärkeänä nähtiin se, että koulutuksen järjestäjä solmii koko mahdollisen alihankintaketjunsa ja esimerkiksi mahdollisten satunnaisesti töitä tekevien kouluttajien kanssa samanlaiset salassapitosopimukset kuin henkilöstönsä jäsenten kanssa. Avainhenkilöriskejä pidetään hyvin yleisenä riskinä henkilöstömäärältään pienissä organisaatioissa. Tältä osin organisaatio X ei poikkea yleisessä tietoturvallisuuden teoriassa kuvatusta tilanteesta. Tiedon kriittisyyden järjestelmällistä määrittelyä ei pidetty käyttökelpoisena henkilöstötietoturvallisuuden hallintakeinona. Harjoittelua avainhenkilöriskien hallintakeinona ei pidetty toiminnan luonteen johteesta mielekkäänä tai tarpeellisena.

Ohjeistus, koulutus ja tiedotus tietoturvallisuuteen liittyvistä asioista nähtiin tärkeiksi. Tosin nämä tietoturvallisuusasiat ovat toteutettavissa vasta sen jälkeen, kun suojattava tieto on määritelty ja tunnistettu. Kattavan, vaikuttavan ohjeistuksen laatimista vaikeuttaa se, että monesti suojattavaa (esimerkiksi luottamukselliseksi luokiteltavaa) tietoa pääsee monessa tapauksessa syntymään ikään kuin vahingossa kehittämis- tai palaveritöiden yhteydessä kesken operatiivisen toiminnan. Myös koulutuksen järjestäjän näkökulmasta on tärkeää, että ohjeistuksen pohjalla toimii kirjoitettu politiikka joka asettaa raamit ja tahtotilan organisaation tietoturvallisuustasolle. Tietoturvallisuuskoulutusta tulisi järjestää rekrytoinnin yhteydessä, mutta henkilöstön kouluttaminen tietoturvallisuusasioissa toistuvasti katsottiin tarpeettomaksi.

Hyväksyttävän käytön säännöillä on koulutuksen järjestäjän näkökulmasta kaksi eri ulottuvuutta. Toisaalta esimerkiksi asiakkaiden ja henkilöstön jäsenten henkilötietojen luottamuksellisuus sähköpostin käytön yhteydessä on jo useita vuosia tiedostettu osaksi tietoturvallisuutta. Toisaalta aiheiden, joita kouluttamalla organisaatio toimii, luottamuksellisuus on usein vaikeasti hahmotettava asia. Opetettavat asiat itsessään eivät monessakaan tapauksessa muodosta luottamuksellisia asiakokonaisuuksia. Sen sijaan esimerkiksi koulutuksen organisointiin liittyvät tiedot voivat vääriin käsiin joutuessaan aiheuttaa haittaa organisaatio X:n toiminnalle. Esimerkiksi sosiaalisen median hyväksyttävässä käytössä on monelta osin tarkennettavaa myös koulutuksen järjestäjälle. Hyväksyttävän käytön sääntöjen määrittely on tärkeää, sillä monesti niin organisaation johto kuin henkilöstön jäsenetkin pitävät itsestään selvyytenä käsiteltävien asioiden luottamuksellisuutta, vaikka käytännössä ei tiedetäkään, mitä sopii julkaista sosiaalisessa mediassa ja mitä ei. Hyväksyttävän käytön sääntöjen laatimista pidettiin tarpeellisena mutta samanaikaisesti tiedostettiin niiden noudattamisen valvonnan vaikeus. Sääntöjen tulisi olla riittävän yleisiä, sillä jokaiselle järjestelmälle omat säännöt muodostavat liian suuren määrän erilaisia säännöstöjä miellettäviksi.

Tietoturvaohjeiden noudattamisen valvontaa pidettiin ongelmallisena valvoa muutoin kuin teknisin keinoin. Käytännössä ainoaksi valvonnan keinoksi tunnistettiin reagointi paljastuneisiin rikkeisiin. Rikkomuksista seuraavat sanktiot kannattaa pitää tapauskohtaisina jolloin vältytään ylireagoinneilta ja vaikutukseltaan liian pieneltä sanktiokäytännöltä. Yrityksen omaehtoinen tutkinta nähtiin organisaatiossa olevalla osaamisella vaikeaksi toteuttaa.

Suhde organisaation ulkopuolisiin työtekijöihin, asiakkaisiin ja vierailijoihin tunnistettiin ongelmalliseksi. Koulutuksen järjestäjällä on toimitilat, joissa se myös järjestää opetusta. Näin ollen on mahdotonta kulunvalvonnan keinoin määritellä kaikkia tiloja ulkopuolisilta pois rajatuksi alueeksi. Henkilöstön toimintaa vieraiden ja muiden ulkopuolisten henkilöiden kanssa tulisi ohjeistaa. On erotettava toisistaan tilat, jotka ovat ainoastaan organisaation oman henkilöstön käyttöön.

KATAKRI:n ulkopuolisista tietoturvallisuuden näkökulmista korostui henkilötietojen suojaamiseen liittyvät kysymykset, joista huolehtiminen on jokaiselle organisaatiolle lakisääteinen tehtävä. Tämän korostumisen perusteella on tarkoituksenmukaista yhdistää henkilöstötietoturvallisuus ja henkilötietoihin liittyvä tietosuoja samaan tarkistuslistaan käytettävyyden lisäämiseksi.

5 Henkilöstötietoturvallisuuden tarkistuslista koulutuksen järjestäjälle

Henkilöstötietoturvallisuuden tarkistuslista laadittiin organisaation X:n kehitystyön työkaluksi organisaation käytettäväksi organisaation oman harkinnan mukaan. Tarkistuslistaa voidaan käyttää auditointityön tukena sekä henkilöstötietoturvallisuuden vähimmäistason saavuttamiseksi. Tarkistuslista on laadittu hyödyntäen kappaleessa 3.3. kuvattua asiantuntijatyötä sekä kirjallisuudesta kerättyä teoriatyötä hyödyntäen.

Henkilöstöturvallisuuden tarkistuslista oli tämän opinnäytetyön toiminnallinen tuote sekä alkuperäinen toimeksiannon välineellinen tavoite. Varsinainen tavoite oli orientoida kohdeorganisaation johto ja avainhenkilöstö opinnäytetyön käsittelemään aihealueeseen, henkilöstötietoturvallisuuteen.

Tarkistuslista löytyy opinnäytetyön liitteistä. Lista toimii organisaatio X:n toiminnan tukena sen omasta harkinnan ja päätösten mukaan. Tähän dokumenttiin on listattu ainoastaan tarkistuslistan sisältämät tarkastelussa hyödynnettävät kysymykset ja niiden kategorisointi. Opinnäytetyöhön ei ole liitetty tarkistuslistan oikeaa graafista ulkoasua, sillä tämä paljastaisi kohdeorganisaation identiteetin. Liitteessä 1 esiintyvien kysymysten lisäksi tarkastuslista sisältää kunkin kysymykset alapuolella seuraavat organisaation muistiinpanoja varten varatut tyhjät tilat:

- Kyllä
- Ei
- Kuka vastaa
- Deadline

6 Yhteenveto ja johtopäätökset

Opinnäytetyöprosessin aikana tunnistin ja otin käyttöön ”henkilöstötietoturvallisuus”-käsitteen. Käsite syntyi tarpeeseen, jonka muodosti erilaisten lähikäsitteiden, kuten henkilöturvallisuus, tietoturvallisuus ja henkilöstöturvallisuus osittainen päällekkäisyys. Henkilöstö-

tietoturvallisuudella tarkoitan sellaista tietoturvallisuutta, joka käsittää henkilöstön toiminnan suojattavan tiedon parissa.

Henkilöstötietoturvallisuuden painopistealueet sekä tarpeet organisaatiossa X eroavat yleisestä tietoturvallisuuden hallinnasta joiltakin osin. Koulutuksen järjestäjää sitoo tietoturvallisuuden näkökulmasta sen palveluihin keskittyvä toimintalogiikka. Usein suojattava tieto muodostuu rahallisesti vaikeasti arvotettavista palveluista sekä yhteiskunnallisesti tärkeästä tiedosta. Lisäksi koulutuksissa eteenpäin jaettavan tiedon luonne ja julkisuusaste vaikuttavat siihen, miten keskeisessä asemassa tietoturvallisuus koulutusten järjestäjän kannalta on.

Ideaalitilanne on sellainen, jossa tietoturvallisuuteen liittyvät riskit ovat lainsäädännön vaatimalla tasolla ja mahdolliseen liiketoimintaan liittyvät konseptit pysyvät organisaation omassa tiedossa. Lähtökohtaisesti kaikki operatiivisessa toiminnassa – eli koulutuksissa – käytettävä tieto, jota viranomaiset eivät ole luokitelleet salatuiksi tai suojatuiksi tulisi olla julkista. Koulutuksen järjestäjän kilpailuetu koulutusmarkkinoilla ei muodostu yksinomaan tiedosta, vaan tiedon, taidon ja asenteen muodostamasta yhdistelmästä. Voidaan siis todeta, että tietoturvallisuus nojautuu vahvasti henkilöstön toimiin ja ratkaisuihin samanaikaisesti kun henkilöstön itsensä pitäisi ihanteellisessa tilanteessa tehdä tietoturvallisuus tarpeettomaksi.

Opinnäytetyön suurin ansio on se, että kohdeorganisaatioon saadaan yhteneväinen terminologia tietoturvallisuuteen sekä saadaan pohja henkilöstötietoturvallisuuden kehittämistyölle. Tietoturvallisuuspolitiikka on keskeinen tekijä tietoturvallisuuden hallinnassa, mutta sen lisäksi kehittämistyö tarvitsee konkreettista työtä joka perustuu tietoturvallisuuden parhaisiin käytäntöihin. Avainasemassa ovat suojattavan tiedon määrittely, lainsäädännön vaatimusten täyttäminen sekä henkilöstön kouluttaminen ja orientointi tiedon suojaamiseen. Kirjallisten ohjeiden laatiminen jokaiseen henkilöstötietoturvallisuuden osa-alueeseen ei itsessään takaa tietojen turvallista käsittelyä.

Opinnäytetyötä ohjaava apukysymys oli ”Miten organisaatio X voi kehittää henkilöstötietoturvallisuuttaan?” Vastaus voidaan kiteyttää seuraavasti: Suojattavan tiedon määrittelyllä sekä varmistamalla, että henkilöstötietoturvallisuuden tarkistuslistassa esiintyvät näkökulmat on huomioitu toiminnan organisoinnissa, voidaan organisaation kokonaisturvallisuutta parantaa merkittävästi.

Lähteet

ASIS. 2007. Information asset protection – Guideline. Yhdysvallat: ASIS.

British Standards Institution. 1995. Information Security Management. Iso-Britannia: BSI.

Heliö, E. 2010. Turvallisuusjohtajan esitelmä Finnsecurity ry:n järjestämässä tietoturvallisuuden aamiaisseminaarissa 28.9.2010. Tieto Corporation. Espoo.

Heljaste, J. 2008. Tietoturvallisuus. Osana teosta: Yrityksen turvallisuusopas. Helsinki: Kauppakamari.

Hirsjärvi, S., Hurme, H. 2008 Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2004. Tutki ja kirjoita. Helsin-ki: Tammi.

International Standards Organization. 2007. ISO 27000-standardiperhe. Ranska: ISO.

Kangas, A. 2009. Yritysten tietoturvallisuus vaarantuu vuorovaikutustilanteissa. Artikkeli osana Suomen turvallisuusalan vuosikirjaa 2009-2010. Forssa: Paulapress.

Krutz, R., Vines, R. 2003. Tietoturvallisuussertifikaatti CISSP. Helsinki: Edita Prima.

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. Helsinki: WSOY.

Laki sopimattomasta menettelystä elinkeinotoiminnassa 22.12.1978/1061.

Laukkala, H. 2010. Standardit ja mallintaminen yrityksen kansainvälisen riskienhallinta- ja turvallisuustyön ohjaajina – missä mennään, mitä kokemuksia? Esitelmä Yritysturvallisuuden neuvottelupäivillä 5.5.2010. M/S Silja Serenade.

Miettinen, J. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari.

Miettinen J. 2002. Yritysturvallisuuden käsikirja. Helsinki: Kauppakaari.

Mustonen, J. 2008. Toimitilaturvalllisuus. Osana teosta: yrityksen turvallisuusopas. Helsinki: Kauppakamari.

Mäkinen, K. 2007. Organisaation strateginen kokonaisturvallisuus. Helsinki: Edita Prima.

Opetushallitus. 2008. Ammatillisen koulutuksen laadunhallintasuositus. Helsinki: Yliopistopaino.

Organisaatio X. 1.6.-28.10.2010. Asiantuntijahaastattelut sekä palaverityö opinnäytetyöhön liittyen. Uusimaa.

Parker, D. 2002. Toward a new framework for information security. Osana Bosworth, Seymour, Kabay, M.E. The Computer security handbook (4th edition). New York: John Wiley & Sons.

Puhakainen, P. 2009. Aktivoi koulutettavan oma ajattelu, herätä turvallisuus innostus. Artikkeli osana Suomen turvallisuusalan vuosikirjaa 2009-2010. Forssa: Paulapress.

Puolustusministeriö. 2009. Kansallinen turvallisuusauditointikriteeristö. Helsinki: Puolustusministeriö.

Sisäasiainministeriö. 2010. Oppilaitosten turvallisuus – työryhmän raportti. Helsinki: Sisäasiainministeriö.

Suomen kielitoimisto. 2010. Puhelinsoitto kielenhuollossa neuvovaan puhelinpalveluun 7.10.2010. Helsinki.

Suominen, A. 1999. Riskienhallinta. Vantaa: WSOY.

Synott, W., Gruber, W. 1981. Information resource management – Opportunities and strategies for the 1980's. New York: Wiley.

Työsopimuslaki 26.1.2001/55.

Valtionvarainministeriö, valtionhallinnon tietoturvallisuuden johtoryhmä. 2004. Valtionhallinnon keskeisten tietojärjestelmien suojaaminen. Helsinki: Edita Prima.

Valtionvarainministeriö, valtionhallinnon tietoturvallisuuden johtoryhmä. 2006. Henkilöstön tietoturvaohje. Helsinki: Edita Prima.

Valtionvarainministeriö, valtionhallinnon tietoturvallisuuden johtoryhmä. 2007. Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Helsinki: Edita Prima.

Valtionvarainministeriö (a), valtionhallinnon tietoturvallisuuden johtoryhmä. 2008. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Helsinki: Edita Prima.

Valtionvarainministeriö (b), valtionhallinnon tietoturvallisuuden johtoryhmä. 2008. Valtionhallinnon tietoturvasanasto VAHTI 8/2008. Helsinki: Edita Prima.

Vapaavuori, T. 2005. Yrityssalaisuudet ja salassapitosopimukset. Helsinki: Talentum.

Vilkka, H. Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Sähköiset lähteet

Elinkeinoelämän keskusliitto EK. 2009. Yritysturvallisuus. Viitattu 25.10.2010. http://www.ek.fi/ytnk08/fi/yritysturvallisuus.php

Jyväskylän yliopisto – verkkosivut. 2010. Tietoturvallisuus osaksi koulujen turvallisuutta. Viitattu 2.9.2010. https://www.jyu.fi/ajankohtaista/arkisto/2010/08/tiedote-2010-08-04-10-03-35-798552

Keksintösäätiö. 2010. Salassapitosopimus. Viitattu 10.10.2010. http://www.keksintosaatio.fi/Ideoijalle/Ideasta-liiketoiminnaksi/Keksinnon-myynti/Lisensointi/Sopimustietoa/Salassapitosopimus/

Korkeakoulujen arviointineuvosto. 2010. Auditointeja koskevat julkaisut. Viitattu 2.9.2010. http://www.kka.fi/index.phtml?s=79

Opetushallitus. 2002. Malli internetin hyväksyttävän käyttämisen säännöistä kouluille. Viitattu 19.10.2010. http://www.edu.fi/materiaaleja_ja_tyotapoja/tvt_opetuksessa/internetin_turvallinen_kaytto/internetin_asianmukainen_kaytto/internetin_kayttaminen_koulussa/malli_saannoista

Opetushallitus. 2010. Rahoitus – Tietoa järjestelmästä. Viitattu 1.9.2010. http://www.oph.fi/rahoitus/valtionosuudet/tietoa_jarjestelmasta

Skurnik, H. 2004. Liikesalaisuuksien suojaaminen. Viitattu 10.10.2010. http://www.helsinki.chamber.fi/index.phtml?1262_m=1270&1262_o=20&s=156

Tietoturvallisuus. 2010. Valtionvarainministeriö – Verkkosivut. Viitattu 2.9.2010. http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp

Tilastokeskus. 2010a. Käsitteet ja määritelmät – Koulutuksen järjestäjä. Viitattu 8.11.2010. http://www.stat.fi/meta/kas/koulutuksen_jar.html

Tilastokeskus. 2010b. Käsitteet ja määritelmät – Koulutussektori. Viitattu 8.11.2010. http://stat.fi/meta/kas/koulutussektori.html

Tilastokeskus. 2010c. Käsitteet ja määritelmät – Oppilaitos. Viitattu 8.11.2010. http://www.stat.fi/meta/kas/oppilait.html

Valtioneuvosto. 2010. Kiinnostuksesta kysynnäksi ja tuotteiksi – Suomen koulutusviennin strategiset linjaukset. Valtioneuvoston periaatepäätös 29.4.2010. Viitattu 2.9.2010. http://www.minedu.fi/export/sites/default/OPM/Koulutus/artikkelit/koulutusvienti/liitteet/Kouutusvienti_VN_suomi.pdf

VTT. 2010. PK-yritysten riskienhallinta - Mitä riskienhallinta on?. Viitattu 6.10.2010. http://www.pk-rh.fi/startti-riskienhallintaan/mita-riskienhallinta-on

VTT. 2010. PK-yritysten riskienhallinta – Avainhenkilöiden työmotivaatio. Viitattu 10.10.2010. http://www.pk-rh.fi/riskilajit/henkiloriskit/avainhenkilot/avainhenkiloiden-tyomotivaatio

VTT. 2010. PK-yritysten riskienhallinta – Avainhenkilöt. Viitattu 10.10.2010. http://www.pk-rh.fi/riskilajit/henkiloriskit/avainhenkilot/avainhenkilot/

Yleisradio. 2010. Salassapitosopimukset leviävät yhä useammille aloille. Verkkopalvelussa julkaistu uutinen 01.07.2010. Viitattu 10.10.2010. http://yle.fi/uutiset/kotimaa/2010/07/salassapitosopimukset_leviavat_yha_useammille_aloille_1798445.html?origin=rss

Liite 1: Henkilöstötietoturvallisuuden tarkistuslista koulutuksia järjestävälle organisaatiolle

Henkilöstötietoturvallisuus - tarkistuslista koulutuksia järjestävälle organisaatiolle

- Onko organisaatio määritellyt, mitkä tiedot ovat suojattavia?
- Tunteeko henkilöstö edellisessä kohdassa tarkoitetut tiedot?

Pääsy- ja käyttöoikeuksien hallinta

- Onko organisaatio tunnistanut, mitkä sen järjestelmistä sisältävät suojattavaa tietoa?
- Millä perusteella henkilöstölle myönnetään käyttöoikeuksia em. Järjestelmiin?
- Katselmoiko järjestelmän/järjestelmien pääkäyttäjä(t) käyttöoikeudet määräajoin haamukäyttäjien poistamiseksi?

Salassapitosopimukset

- Ymmärtääkö henkilöstö salassapitosopimusten asettamat luottamuksellisuusvaatimukset?
- Mitä osa-alueita salassapitosopimukset kattavat?
- Onko vahingonkorvausvastuu määritelty koulutusorganisaation tarpeita vastaavaksi?
- Koskevatko salassapitosopimukset myös koulutusoperaatiossa käytettäviä alihankkijoita, väliaikaista työvoimaa, vierailevia luennoitsijoita jne?

Avainhenkilöjärjestelyt

- Onko avainhenkilöriskit tunnistettu?
- Onko koulutusoperaatio suunniteltu siten, että se kestää kenen tahansa avainhenkilön poistumisen organisaation palveluksesta?
- Onko ns. vaaralliset työnkuvayhdistelmät tunnistettu ja poistettu?

Ohjeistus, koulutus ja tiedotus

- Onko olemassa menettelyohje tilanteeseen, jossa suojattavaa tietoa pääsee muodostumaan ennakoimatta esimerkiksi ideointipalaverin tuloksena?
- Hallitseeko henkilöstö em. menettelyt?
- Järjestetäänkö henkilöstölle tietoturvallisuuskoulutusta rekrytoinnin yhteydessä?

Hyväksyttävän käytön säännöt

- Onko henkilöstölle määritelty, mihin tarkoitukseen yrityksen tietojärjestelmiä saa hyödyntää?
- Onko organisaatiossa arvioitu, millaisen riskin kunkin tietojärjestelmän väärinkäyttö voi pahimmillaan aiheuttaa?
- Onko henkilöstölle määritelty, mitä töihin liittyviä asioita sosiaalisessa mediassa saa TAI ei saa ilmaista?

Ohjeiden noudattaminen ja sen valvonta

- Reagoidaanko organisaatiossa tapahtuneisiin tietoturvarikkomuksiin?
- Onko tietoturvarikkomuksista seuraavat rangaistukset määritelty?

Ulkopuoliset työntekijät ja vierailijat

- Onko organisaation tilojen julkisuusaste määritelty?
- Onko henkilöstö tietoista tilojen julkisuusasteista?
- Noudatetaanko organisaatiossa "puhtaan pöydän politiikkaa"?
- Onko ulkopuolisten henkilöiden pääsy ei-julkisiin tiloihin estetty?
- Onko organisaatiossa menettely vierailutilanteisiin, tunteeko henkilöstö ne ja noudatetaanko niitä?

Henkilöstö henkilötietojen käsittelijänä

- Tietääkö henkilöstö, mitkä henkilötiedot ovat salassa pidettäviä?
- Tunteeko henkilöstö vastuunsa henkilötietojen käsittelyssä?
- Onko olemassa menettelyohjeet tilanteeseen, jossa henkilötietoja on joutunut / epäillään joutuneen vääriin käsiin?

Liite 2: Asiantuntijahaastattelussa käytetty pohja

1. Kerro omin sanoin, mikä on tiedon merkitys koulutuksia järjestävän organisaation toiminnalle.
2. Mitkä ovat organisaatiossasi keskeisiä huomionkohteita henkilöstöön liittyvässä tietoturvallisuudessa?
3. Kerro ovatko seuraavat henkilöstötietoturvallisuuteen liittyvät asiat koulutuksen järjestäjälle relevanttia tietoa ja jos on, millä perusteella?
    a. Pääsy- ja käyttöoikeuksien hallinta
        i. Näetkö tarpeellisena (perustelut):
            1. myöntäminen tarpeen perusteella
            2. katselmointi
            3. oikeuksien myöntäminen vain niitä tarvitseville
            4. oikeuksien myöntämisen ja poistamisen dokumentointi
    b. Salassapitosopimukset
        i. näetkö tarpeellisena(perustelut):
            1. vahingonkorvausvelvoitteen määrittelyn
            2. määräajan
            3. alihankintaketjujen ja sidosryhmien sisällyttämisen sopimusten piiriin
    c. Avainhenkilöjärjestelyt
        i. Näetkö tarpeellisena(perustelut):
            1. avainhenkilöiden määrittelyn
            2. tiedon kriittisyysasteen määrittelyä
            3. varamiesjärjestelyt
            4. harjoittelun poikkeustilanteita varten
            5. vaarallisten työyhdistelmien tunnistamisen ja poistamisen
    d. Ohjeistus, koulutus ja tiedotus
        i. Näetkö tarpeellisena (perustelut):
            1. ohjeistuksen perustumisen politiikkaan tai muuhun raamiin
            2. ohjeistuksen olemassaolon
            3. ohjeistuksen koulutuksen
            4. koulutuksen järjestämisen (kerran vai useammin?)
            5. poikkeamista ilmoittamisen & ohjeistuksen tähän
            6. tiedottamisen henkilöstölle?
    e. Hyväksyttävän käytön säännöt
        i. Näetkö tarpeellisena (perustelut):
            1. sääntöjen laatimisen
            2. sääntöjen noudattamisen valvomisen
            3. sääntöjen järjestelmäkohtaisuuden vai sääntöjen yleisluontoisuuden?
            4. erottamisen muista tietoturvaohjeista
    f. Tietoturvaohjeiden noudattaminen ja rikkomukset
        i. Näetkö tarpeellisena (perustelut):
            1. ohjeiden noudattamisen valvonnan
            2. sanktioiden määrittelyn vakioiksi / tapauskohtaisiksi
            3. yrityksen omaehtoisen tutkinnan järjestämisen
    g. Ulkopuoliset työntekijät ja vierailijat
        i. Näetkö tarpeellisena (perustelut):
            1. ohjeistuksen

2. menettelyt
3. toimitilaturvallisuuden korostamisen